UNIVERSITY OF NAIROBI

SCHOOL OF COMPUTING AND INFORMATICS

A FRAMEWORK FOR IMPROVEMENT OF INFORMATION SECURITY IN PUBLIC FINANCING INSTITUTIONS:

THE CASE OF HIGHER EDUCATION LOANS BOARD (HELB)

PAUL OBIERO OLANG

In Partial Fulfillment of the Requirements for the Degree of Master of Science (Information Systems)

July 2013

DECLARATION

This research project is my original work and has not been submitted for the award of a degree in any other university.

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

Paul Obiero Olang

Reg. No.: P56/P/7371/2005

This research project has been submitted for examination with my approval as university supervisor.

Signed: …………………………………………… Date: …………………………

Mr. Joseph Ogutu

Lecturer,

School of Computing and Informatics

DEDICATION

I dedicate this work to my wife Carole and son Trevor for their support during its preparation.

ACKNOWLEDGEMENT

The contributions of many different people, in their different ways, have made this possible.

First, I would like to thank God for the wisdom and perseverance that He has bestowed upon me during this research project, and indeed, throughout my life.

Second, I offer my sincere gratitude to my supervisor; Mr. Joseph Ogutu who has supported me throughout this research project with patience and knowledge whilst allowing me room to work in my own way.

I wish to thank all the respondents who participated in this study and all those agreed to critic my work you have been a source of strength.

ABSTRACT

The use of information and communication technologies has improved the efficiency and flexibility in providing services to various sectors of the economy, while appreciating the fast speed of these developments; organizations are faced with wide range of challenges amongst them the threats on the information and information assets, making securing information a crucial function within the information management

The purpose of this study was to examine information security and to investigate the factors that influence the level of information security in public financing institutions in Kenya and to propose a framework for improving the level of information security. Through literature review, the study presents factors that affect level of information security as organizational, human, socio-cultural, technological and external environmental factors; the study further establishes the level of information security. The study was conducted at Higher Education Loan Board and employed descriptive research design on sample size of 68 without putting into consideration the population and assuming a probability of 50/50. A single case study approach to analyze the responses to self-administered closed-ended questions constructed based on conceptual framework and results presented in tables, graphs and pie-charts. Results indicate through multiple regression analysis that there is a positive and significant relationship between all the five factors that influence the level information security. It is also evident that organizations implement information security partially as the study recommends evaluation of information security and comprehensive implementation.

KEY WORDS: information security level, organizational factors, external environmental factors, socio-cultural factors, human factors

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF ABBREVIATIONS

ANOVA	Analysis of Variance
AFC	Agricultural finance Corporation
CCK	Communications Commission of Kenya
COBIT	Control Objectives for Information and Related Technology
CoDF	Coffee Development Fund
COSO	Committee of Sponsoring Organizations of the Treadway Commission
GOK	Government of Kenya
HELB	Higher Education Loans Board
HELF	Higher Education Loans Fund
ICT	Information and Communication Technology
IEC	International Electrotechnical Commission
ISF	The Information Security Forum
ISMSs	Information Security Management Systems
ISO	International Organization for Standardization
ITIL	Information Technology Infrastructure Library
SLA	Service level Agreement
PWC	Price Waterhouse Coopers
WEF	Women Enterprise Fund
SPSS	Statistical Product and Service Solutions

CHAPTER ONE:

INTRODUCTION

1.0 Background of the Study

Organizations are today dependent on their information technology resources, not only for their survival but also for their growth and expansion in today's highly competitive global markets both in public and private institutions (Von Solms, 1999). However, organizations face a wide range of information threats, securing their information has become a crucial function within the information system management, and with the increase on reliance on technologies connected over open data networks, effective information security management has become a critical success factor.

Information security is the protection of information from a wide range of threats in order to ensure business continuity, minimize business risk, and maximize return on investments and business opportunities (ISO/IEC 27001: 2005). For effective management of information security in organization, Information Security Management Systems (ISMSs) are developed. ISMS manage and operate continuously information security system, in terms of technology, management, and hardware, for the aim of the information security that is to achieve confidentiality, integrity, and availability. Information security maintains three basic services:

i. Confidentiality of sensitive information, which is concerned with preventing disclosure of information to unauthorized users.
ii. Integrity, which is concerned with ensuring that data cannot be modified without authorizations.
iii. Availability, which is concerned with ensuring information must be available to authorized users when they require them

It is no longer possible to rely entirely on our traditional security controls e.g. physical access controls, security guards to ensure the security of an organization's assets, processes and communications (Tarimo, 2006). The multiplicity of new technical possibilities has given rise not only to new products, services and more efficient and effective way of doing things, but also the possibility of misuse of the technologies. However, research findings show that, in many cases, security issues come as an-after-thought in the ongoing transformation to ICT-enabled organizational or governmental context (Tarimo, 2006).

PriceWaterHouseCoopers (PwC) (2011) noted that Global Cyber Security spending was expected to reach $60 billion in 2011 and is forecast to grow at 10 percent every year during the next three to five years. The U.S. accounts for more than half of all deals globally triggered by growing cyber threats and increasing awareness among both organizations and consumers of accelerating breaches and attacks. Since 2008, the total investment in global Cyber Security deals has exceeded $22 billion, an average of over $6 billion in each year.

In most regions, the private sector accounts for the majority of Cyber Security spending, while the U.S. is the only notable exception to this trend where government spending is almost equal to the private sector. The strong U.S. technology industry combined with the fact that the U.S. defense and intelligence budgets are significantly larger than in any other country are key market drivers.

1.0.1 Current Concerns about Information Security in Kenya

Vision 2030 identifies ICT as one of the core drivers of Kenya's growth and development strategy to becoming a middle income country by 2030. To realize this, the Government is at the moment investing heavily in ensuring that the entire country has access to internet services at an affordable cost. Government is heavily investing in fibre optic cables at least to every provincial headquarters as well as providing means for investors to lay fibre cables as well and has an ambitious plan to have all urban centres connected to the worldwide web. Although the Government of Kenya has for quite some time now placed a high premium on the efficiency of ICT as a development catalyst, it has not yet fully exploited the potential of the sector in part due to the current inadequacy of ICT infrastructure (GOK, 2008). Part of the reasons for low investment in ICT is that ICT programs are known to have high failure rate. Heeks (2003) asserts that 35% of ICT programs are regarded as total failures and 50% as partial failures in the government. One of the most common cited reasons for this failure is ICT security problems. Other reasons are associated with resource gaps, cultural gaps, infrastructural gaps and leadership/steering gaps (Heeks, 20003)

Nalika (2011) argues that three years ago Internet connectivity was a major concern in Kenya, until the undersea optical fiber cable linking the country to the world was commissioned. This connectivity has enabled business to collaborate with overseas partners among other benefits, though the super highway has brought yet another problem - Cyber security. This has shifted the priority of the Kenyan government to create awareness and secure virtual systems operating in the internet ecosystem.

Kenya's internet infrastructure is not safe from online fraudsters and other malicious cyber crooks (Nyabiage, 2011). As the country boasts of three undersea fibre optic cables, cyber-attacks are on the rise, targeting the Government and corporates with rich databases. On the first week of January 2011, the Kenya Police website was taken over by cyber criminals, twice. The website was not a stranger to getting hacked, and has been a popular target. Other government websites have also been popular hacking targets. This raises the question on the safety of data held by the Government, as the country continues to adopt e-government strategies. Recently, the ministry of Finance's website was brought down. In January 2011GoK and other department like statehouse and AP sites were among the sites hacked, and also mobile phone company YU's, among others that were also victims. When the government's website was hacked into, it was turned into a promotion portal for Viagra, the sex enhancing drug.

The moment the first submarine fibre optic cable landed at Kenyan Coast, local businesses became more accessible on the World Wide Web (www), attracting the attention of international hackers. The tragedy is local businesses did not move with speed to upgrade information security systems to ward off international hackers. These companies are now prone to hefty financial losses through theft or data corruption.

Mwale (2011) of Technology Partners Ltd argues that the country lacks measures and policies to keep off cyber criminals. The biggest problem in many organisations is a weak human resource structure. You will get that 80 per cent of hacking is due to human resource failure. There is always insider help and lack of oversight. This should be considered as a wake-up call for organizations to take internet and information security seriously. More of this will be seen as more youth acquire hacking skills (Mwale 2011)

Ngundi (2010) argues that more than 80 per cent of websites in Kenya and the region are vulnerable to hackers. In addition, Kenya has put in place various provisions to enhance the management of cyber security. Provisions enshrined in the Kenya Communications (Amendment) Act of 2009 which mandates the Communications Commission of Kenya (CCK), Kenya's national ICT Regulatory Authority, to develop a national electronic transactions framework.

PriceWaterHouseCoopers (PwC) (2011) asserts that Kenya is among several countries ranked high in terms of fraud in the world, though cyber-attacks are minimal because most of the country's records are not digitized. The report points out that 40% of cyber problems emerge from internal employees of an organization. Therefore, companies need to educate their employees on measures of protecting company information and instilling a sense of discipline in terms of information security.

1.0.2 Comparison of Information Security in Private and Public Financial Institutions

The main aims of commercial organizations is to improve shareholder value, while in public financing institutions the main objective is to meet the organization's missions such as business continuity, deliver quality services, minimize business interruption, eliminate fraud and corruption, minimize loss of property, protect copyright, ensure privacy, ensure confidentiality and minimize consequential liabilities, protect organization's reputation, etc. The ability of any organization to achieve its mission and meet its business objectives is directly linked to the state of its computing infrastructure. Although in public financing institutions the main objective is not to a make profit, risks associated with information do have financial implications too. Therefore, in order to ensure that, the public financing institutions meet their objectives, there must be an insurance structure which encompasses insurance policies such as information security policies, standards, guidelines, codes-of-practices, technologies, legal and ethical issues to counter the risks associated with information.

When a commercial organization makes losses, they make decisions on business grounds such as closing the company among others. However, closing public financing institutions like HELB or a government ministry for the loss associated with the information system risks is not practical and one of the measures public institutions can take is to estimate the loss, which in most cases might be associated with the cost of reactivating the affected services. Another way is estimate the loss by also associating it with the cost of putting the service right so that particular problem does not happen again as well as working out the estimates associated with those who are affected by the absence of the system.

1.0.3 Public Financing Institutions

These are government owned institutions mandated to offer credit in the form of loans, equity positions to the public, these institutions have a general responsibility to provide finance for investment that promote development in areas where the market fails to invest sufficiently. Examples of public financing institutions include Higher Education Loans board (HELB), Coffee Development Fund (CoDF), Agricultural Finance Corporation (AFC), Women Enterprise Fund (WEF) and Youth Enterprise Fund.

These institutions do their business like commercial banks in term of their operations yet they are not under the direct regulation of the central bank of Kenya as they draw their individual mandates from respective line ministries. Public financing institutions face similar information security threats as banks though the commercial banks are expected through the central bank of Kenya to put in place measure to protect their information, some of the known threats include Malware (viruses, worms, spyware, Trojan horse programs) Social Engineering (Phishing, Whaling, Pharming, Dumpster Diving), Mobile devices, Data Loss, Internet attacks

1.0.4 Higher Education Loans Board

The genesis of student loans in Kenya dates back to 1952, when the government, then British colonial, set up the Higher Education Loans Fund (HELF) to assist those pursuing university education outside East Africa mainly in Great Britain, the USA, India, the USSR, and South Africa. On attaining independence, the African government more or less suspended the scheme and opted to directly meet the costs of higher education (Otieno, 1997).

This policy was in line with the recommendation of the Kenya Education Commission to train highly skilled African personnel to take over the running of the government from the departing Europeans (Republic of Kenya, 1964). Subsequent policy documents such as Sessional Paper No. 10 of 1965 on African Socialism and Its Application to Planning in Kenya (Republic of Kenya, 1965a), the first Development Plan, 1965–1970 (Republic of Kenya, 1965b) as well as the report on High Level Manpower Requirements and Resources in Kenya, 1964–1970 (Republic of Kenya, 1964) all stressed that high- and middle-level human resources are a critical resource in achieving rapid economic growth and that the production of high-level human resources is one of the goals of university education (Mwiria and Ngethe, 2002)

The government used these arguments as the basis for expanding and subsidizing higher education. University education as such became virtually free to students, as the government bore most of the direct costs. The increased enrollments in university education coupled with dismal economic performance mainly occasioned by the oil shocks of 1970s forced the government to rethink its policies on financing university education. As a result, it introduced a loan program in the 1973–1974 financial year. In reality, it was simply a reactivation of the 1952 program, which had never been formally discontinued; the government had merely stopped funding it. The program was reintroduced as the University Students' Loan Scheme. The 1973 program was not administered by an autonomous body but by the Loan Disbursement and Recovery Unit in the Ministry of Education (Mungai, 1989).

The program was faced with many hurdles. The biggest hurdle was loan recoveries. This led to the introduction of reforms through a new legal body (Higher Education's Loans Board-HELB).

The Higher Education Loans Board was established by an Act of Parliament. The statute known as The Higher Education Loans Board Act, 1995 was legally established as Act number 3 of 1995. It came into existence on the 21st day of July 1995 through Kenya Gazette Supplement (Cap 213A).

The functions of the board are to facilitate the disbursement of loans, scholarships and bursaries to needy Kenyan students. In addition, the board is mandated to recover all outstanding loans given to former university students' since1952 through the Higher Education Loans Fund (HELF). Furthermore, it is mandated with establishing a revolving fund from which funds could be drawn and lent to needy Kenyans pursuing higher education. The government anticipated that this revolving fund would ease national education expenditures, which had been close to 40% of the national budget. The HELB further invests surplus funds in any investments authorized by law and seeks additional funding from other organizations the private sector, philanthropic organizations, foundations. (Cheboi, 2002)

1.1 Problem Statement

A study by Delloite (2011) revealed that organizations in East Africa are ill prepared to detect, prevent and investigate information security breaches. The report further revealed that some common information security barriers include lack of sufficient budgets, skilled professionals, and visibility within the organizations.

In Kenya most financial institutions have tried to establish programs and plans to address their information security needs. However, this has not been sufficient to address the rapidly changing security breaches without incorporating information security frameworks. Again, considering a study by Makatiani (2012) where many Kenyan public institutions have been hacked, clearly demonstrate lack of adequate mechanisms to address this problem.

Based on previous studies it's evident that most financial institutions suffer information system insecurity which affects their general operations and objectives. This study therefore intends to develop a framework for the improvement of information security levels in Kenyan public financing institutions

1.2 Research Objectives

The general objective of this research study is to understand the management of information security in public financing institutions in Kenya; the research involves identifying factors that affect the level of information security with a view of applying them in Kenyan context in order to propose a framework for the improvement information security in public financing institutions in Kenya. In order to achieve the larger goal the specific objectives are:

i. Establish the effect technological factors on the level of information security
ii. Establish the effect external factors on the level of information security
iii. Establish the effect human factors on the level of information security
iv. Establish the effect organizational factors on the level of information security
v. Establish the effect socio-cultural factors on the level of information security
vi. Establish the level of information security at Higher Education loans Board

1.3 Purpose of the Study

The purpose of the study is to investigate the factors influencing information security levels with the intention of formulating a framework for the improvement of information security levels in public financing institutions.

1.4 Research Hypothesis

Ho1: Organizational factors do not influence the level of Information security at HELB?

Ho2: Human factors do not influence the level of Information security at HELB?

Ho3: Technological factors do not influence the level of Information security at HELB?

Ho4: External environmental factors do not influence the level of IS at HELB?

Ho5: Socio-cultural factors do not influence the level of Information security at HELB?

1.5 Significance of Study

The study will be of use to management of information security public financing institutions in Kenya. This is because it will highlight the factors that influence the level of IS security in these institutions. Managers will therefore use these results to develop and validate a framework for improving the IS security levels in the institutions.

The findings of this study will be a value addition to literature. Therefore, students of finance, public management, governance, information technology, human resource management, and law will find this research finding critical in terms of broadening their minds in this area.

CHAPTER TWO:

LITERATURE REVIEW

2.1 Introduction

The entire chapter reviews the literature related to the key study variables as depicted in the conceptual framework. The chapter also looks into the linkages in addition to establishing the existing relationships amongst these variables. Empirical studies as relates to the study variables are reviewed in the chapter in order to lay down ground for research. The chapter also attempts to justify the study in addition to reinforcing and underpinning the conceptual framework.

2.2 Theories and Models for Information Security

This section identifies the various framework of information security in an effort to identify the important components that can be used for developing a tailor made framework for improving Information security in public financing institutions in Kenya.

2.2.1 The role of standards and frameworks

Information security standards provide the basis for safeguarding organization's valuable information (Von Solms, 1999). As with other quality standards for other industrial processes like for manufacturers and customer care services information security management systems standards and guidelines are already in place to address methodical and certifiable methods that an organization conforms to industry best practice and procedures. The main objectives of the standards are to protect the organization's information assets in the context of confidentiality, integrity and availability. Examples of major standards include COBIT, COSO, ITIL, and ISO/IEC 27001.

Standards and guidelines only provide generic guidance and are not therefore solutions for the management of information security. They are heavily reliant on organizations risk analysis to determine how they should be implemented and require policy baseline without providing specifications for compliance with the standard (Hone and Eloff, 2002). Standards and guidelines are mainly driven by the needs of the private sector and lack authoritative support in terms of which is the most preferred one for use in practice.

Issues related to public sector require more consideration for instance the organization environment, culture, and diversity of stakeholders, political environment. Standards are usually adopted based upon availability of resources, further more standards will lack legitimacy until they are backed with government decision that enforces the adoption of such standard example is the case of ISO 9001: 2008 Quality management system in Kenya, that require all government departments and ministries to implement the standard for better service delivery. One of the other additional challenges that most organizations encountered is the practical implementation process of these standards as there is shortage of personnel that are competent in implementing information security standards in Kenya.

This study picked important parts from COBIT and ISO/IEC to help come up with a tailor made framework, the basic difference between COBIT and ISO27001 is that ISO 27001 is only focused on information security, whereas COBIT is focused on more general information technology controls. Thus, COBIT has a broader coverage of general information technology topics, but does not have as many detailed information security requirements as ISO 27001

2.2.2 COBIT Security Framework

The purpose of COBIT framework is to provide the management with an IT governance model that helps them control and manage the information and related technology. The Framework explains how IT processes deliver the information that the business needs to achieve its objectives. This delivery is controlled through 34 high-level control objectives, one for each IT process, contained in four domains. The Framework identifies which of the seven information criteria (effectiveness, efficiency, confidentiality, integrity, availability, compliance and reliability), as well as which of the IT resources (people, applications, technology, facilities and data) are important for the IT processes to fully support the business objectives (Hussain and Siddiqui, 2005).

Effective information security requires a comprehensive, integrated set of security, management and governance processes to plan, organize and counter the organization’s information security risks. COBIT provides an integrated governance, management and process framework to implement and execute information security. COBIT describes sound processes, practices, and control objectives for managing and operating IT systems, including their security state. With COBIT framework organizations report an increased ability to deliver high quality service to their customers, which includes being able to measure and satisfy confidentiality, availability, and integrity requirements. COBIT supports security needs to be addressed as a part of every business function. Only one COBIT process (DS5) is specifically devoted to security, control objectives that address security are scattered throughout the various processes in each domain.

2.2.3 ISO/IEC 27001 Standard

ISO/IEC 27001 has its origins from a code of good practice published by the UK department of Trade and Industry in 1989. ISO/IEC 27001 specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented Information Security Management System (ISMS) within the context of the organization's overall business risks. ISO/IEC 27001 specifies requirements for the implementation of security controls customized to the needs of individual organizations or parts thereof. The ISMS is designed to ensure the selection of adequate and proportionate security controls that protect information assets and give confidence to interested parties. The proposed requirements are structured in a classification of 11 clauses that include 39 objectives aimed by 133 controls (ISO/IEC 27001)

ISO/IEC 27001 sets out how a company should address the requirements of confidentiality, integrity and availability of its information assets and incorporate this into an Information Security Management System (ISMS) (Thomson and Solms 2005). ISO/IEC 27001 is used throughout the world by organizations, both commercial and government, as the basis for the management of the organization's policy and implementation of information security. It is being used by small, medium and large organizations across a diverse range of business sectors. In fact the standard is designed to be flexible enough to be used by all types of organization.

The ISO/IEC 27001 standard uses a cyclic model known as the Plan-Do-Check-Act (PDCA) model that establishes, implements, monitors and improves the effectiveness of an organizations ISMS.

2.2.4 Summary of information security baseline standards benefits to organization s

These are a sample of important benefits for baseline standards on how they can help organizations improve, implement and manage information security processes.

i. Standards keep information security business and service focused. Too often, information security is perceived as a cost center or hindrance to business functions. With standards, business process owners and IT negotiate information security services; this ensures that the services are aligned with the business needs.

ii. They enable organizations to develop and implement information security in a structured, clear way based on best practices. Information security staff can move from firefighting mode to a more structured and planned approach.

iii. With its requirement for continuous review, standards can help ensure that information security measures maintain their effectiveness as requirements, environments, and threats change.

iv. They establish documented processes and standards (such as SLAs and OLAs) that can be audited and monitored. This can help an organization understand the effectiveness of its information security program and comply with regulatory.

v. Standards provide foundation upon which information security can be built. It requires a number of best practices - such as Change Management, Configuration Management, and Incident Management - that can significantly improve information security. For example, a considerable number of information security issues are caused by inadequate change management, such as misconfigured servers.

vi. Enables information security staff to discuss information security in terms that other groups can understand and appreciate. Many managers cannot understand low-level details about encryption or firewall rules, but they are likely to understand and appreciate standards concepts such as incorporating information security into defined processes for handling problems, improving service, and maintaining SLAs. Standards can help managers understand that information security is a key part of having a successful, well-run organization.

vii. The organized framework prevents the rushed, disorganized implementation of information security measures. They require designing and building consistent, measurable information security measures into ICT services rather than after an incident. This ultimately saves time, money, and effort.

viii. The reporting associated with standards keeps organization's management well informed about the effectiveness of their organization's information security measures. The reporting also allows management to make informed decisions about the risks their organizations have.

ix. Standards define roles and responsibilities for information security. During an incident, it is clear who will respond and how they will do so.

x. Establishes a common language for discussing information security. This can allow information security staff to communicate more effectively with internal and external business partners, such as an organization's outsourced security services.

2.2.5 Information Security Management (ISM)

Information security is concerned with information properties of confidentiality, integrity and availability. These properties support services such as user authentication, authorization and reliability of information, plus other properties which include authenticity, accountability, non-repudiation, and reliability which are also part and parcel of information security (ISO/IEC 17799:2005)

Information Security Management is therefore the Process that ensures the Confidentiality, Integrity and Availability of an Organization's Assets, information, data and IT Services (ITIL). In public financing institutions business mismanagement of information security can constitute a significant risk to an organization, as they generally hold large volumes of personal and financial data about their customers, such as names, addresses, dates of birth, bank account details, transaction records and PIN.

2.3 Empirical Review

In this section the factors influencing levels of information security in public financing institutions will be highlighted. Factors that influence security in any organization can be grouped in five main categories these includes human factors which relate to cognition at the individual level and interaction with other people, organizational factors these relate to the structure of the organization, including size and managerial decisions around information security, external environmental factors involves the interaction with the outside environment of an organization and technological factors involving technical solutions such as applications and protocols; the last is Socio-cultural factors that involves beliefs, customs, practices and behavior that exists within a population. These factors will further be evaluated to measure the level of security in public financing institutions will in turn show the areas that require improvements apart as well as determine if they influence level of information security.

2.3.1 Organizational factors:

Organization factors are those related to the structure of the organization, and they include size of the institution and management decisions around information security and contain factors like management support, budgetary allocation, information security policy enforcement and adaptation, organizational mission and risk analysis.

2.3.1.1 Management Support – It is the responsibility of management to put in place an environment that allow business to achieve its desired objectives, vision, and mission hence without the management commitments, there will be defects in the operational activities because there decisions drives organization. Management will enforce the implementation of information security initiatives as well as bring information security management with corporate objectives and strategies. The frequent changes in technologies require huge investments in Information Security Management; therefore, managements are in position to make sufficient resources available for the implementation of Information Security in the organization. Previous researchers have demonstrated that management commitment is positively associated with the perceived ease of use of management support of Information Security in the organization (Igbaria et al., 1997). Their studies documented that the commitment and support received from the management is an important factor for managing information security successfully.

2.3.1.2 Budgeting - Without a proper budget, organizations will not be equipped with sufficient resources to ensure that their information resources are secure. Doherty and Fulford (2005) states that organizations require adequate funding to achieve effective information security, Dinnie (1999) further states that lack of information security budgeting in organizations leads to under-investment in appropriate controls. There are essential operating systems, applications and other technologies just to mention a few which are required to support the implementation of information security in the organization (Canavan, 2003). Organizations with lack of proper software or hardware requirements will face difficulties in handling some security issues such as access control mechanisms or helping employees to apply good security practice like an automatic logoff or regular password changes as well as putting programs for awareness.

2.3.1.3 Risk Analysis – Risk analysis is the process of defining and analyzing the dangers to individuals or businesses posed by potential natural and human-caused adverse events. In ICT, a risk analysis report can be used to align technology-related objectives with a company's business objectives. Security risk analysis, otherwise known as risk assessment, is fundamental to the security of any organization. It is essential in ensuring that controls and expenditure are fully commensurate with the risks to which the organization is exposed. Risk analysis must be undertaken on all information systems and intellectual property in the organization. This process aids the organization in determining valuable assets as well as the counter-measures to protect the assets. The risk analysis will specify whether the organization has other specific risks not included in the baseline that need to be addressed. Without risk analysis, Risks can be treated but it will be unknown whether the right risks are being treated and investments cannot be justified is terms of risks they reduce. Without risk analysis, information security is considered to be performed blindly.

2.3.1.4 Information Security Policy - An organizational information security policy is a set of laws, rules, and practices that regulate how an organization manages, protects, and distributes its resources. These laws, rules, and practices must give direction for according individuals authority, and should specify conditions under which individuals are permitted to exercise their authority. To be meaningful, these laws, rules, and practices must provide individuals reasonable ability to determine whether their actions violate or comply with the policy. Without policies, there will be no procedures, countermeasures or controls for an organization to maintain a secure information system and intellectual property. There is no sense in following a policy that does not reflect the security issues of the organization or that is not comprehensive. Through baseline standards concepts, the policies are constructed to ensure that every aspect is covered in the policy document, thereby ensuring a secure information system and intellectual property.

2.3.1.5 Organization Mission - information security in organizations is usually not attended to as long as nothing goes wrong, but when things do go wrong, they suddenly pay attention and a lot of effort is required to recover from the situation, even though sometimes full recovery is impossible. Organization's clear goals and objectives are essential in implementing information security policies and that having a culture of secure information in the organization will affect its success. McKay (2003) clarifies that if the organization's mission is not addressed, the organization will continue to struggle to secure its information and employees will not take responsibility seriously and will not follow and respect the guidelines in the information security policy.

2.3.1.6 Controlling access - is an important challenge for many organizations, this is due to sensitive data distributed in different areas of the organization or to client sites; this data needed to be accessed by stakeholders from different networks and systems and therefore require control. Organizations need to account for all the data they share with third party and agree on responsibility boundaries of information accessed them.

2.3.2 Human Factors

Human factors which relate to cognition at the individual level, and interaction with other people include awareness, and information security training and education

2.3.2.1 Information Security Awareness - This is the proactive measure of making employees aware of how to protect organizational and customer information through the process of information security. A good security awareness program should educate employees about corporate policies and procedures for working with information technology. Employees should receive information about who to contact if they discover a security threat and how to handle confidential information. Regular awareness programs are particularly necessary in organizations especially with high turnover rates and those that rely heavily on contract or temporary staff. Confirming how well the awareness program is working can be difficult but very necessary process to gauge the level of awareness within the organization. Employees of the organization need to know about the policy, its contents and where they can access it.

2.3.2.2 Information Security Training and Education - Awareness is not training. The purpose of awareness presentations is simply to focus attention on security. Awareness presentations are intended to allow individuals to recognize information security concerns and respond accordingly. In awareness activities, the learner is the recipient of information, whereas the learner in a training environment has a more active role. Awareness relies on reaching broad audiences with attractive packaging techniques. Training is more formal, having a goal of building knowledge and skills to facilitate the job performance. Employees need to be educated about the security aspects required in the information security policy. Training is required to build the knowledge of employees and to enable them to put the information security policy into practice. Specific job-related training of business and technical implementation is a requirement not to be overlooked by organizations.

2.3.3 Technological factors

Technological complexity is another challenge for information security management. These complexities make it extremely difficult for the decision makers to manage the big picture and design information security policies that cover all the possible configurations of systems. Technological factors found in literature that affect the level of information security include complexity of systems, mobile and distributed access, and vulnerabilities in systems and applications.

2.3.3.1 System complexity Information systems complexity is a serious concern to information security. From mobile to the cloud and practically everything in between, all businesses have information systems complexities which create big security issues. For example an infrastructure complexity would typical network that has firewalls, proxies, switches behind the firewall, routers in front of the firewalls, mail servers and not enough people to look after the overall security of these interconnected devices. Other factors such as decentralization of ICT management, interaction with other organizations, and distributed sensitive data increases the complexity of technical solutions. These technical solutions need to restrict access from different users with different needs and security requirements.

2.3.3.2 Mobile and distributed user access make it difficult to control access to internal resources. Laptops can be taken to different places and accessed by people who do not have enough technical expertise; these users often come back to the local area network to work with their laptops infected with malicious software from home usage.

2.3.3.3 Access vulnerabilities in systems and applications

There is sensitive data distributed in different areas of the organization, this data needed to be accessed by stakeholders from different networks and systems ie through local LAN, Wireless LAN, VPN, different applications. The main concern is when there is no system to control access to data in a centralized fashion.

2.3.4 Socio-cultural factors

Socio-cultural factors are set of beliefs, customs, practices and behavior that exists within a population, and include socio-ethical awareness, culture and religion

2.3.4.1 Socio-ethical awareness - The concept of socio-ethical information security awareness can be defined as the conforming of an organization to recognized Information Security ethical principles. Principles include privacy, property and obligation. Property of information would, for instance, constitute the right of an individual and an organization to ownership of all information about them or of all information that has been gathered at their expense. Often, property is also protected by law, such as copyright on program code. Privacy of information concerns the right of an individual or an organization to have its information deemed secret. Finally, an organization is obligated to adhere to these socio-ethical information security awareness controls, as well as to follow through on the client’s wishes. The onus rests with an organization to create this socio-ethical awareness in every one of its members and among all its clients and affiliates. Furthermore, it must be the constant endeavor of an organization to incorporate socio-ethical issues with the inception, development and maintenance of its ICT system.

Organizations have obligations towards their customers, other organizations, the community and itself

2.3.4.2 Information Security Culture/Change - When it comes to information security, culture includes the beliefs, values or behavior with regard to security, or the behavior in protecting the information assets of an organization. The Information Security Forum (ISF) defines information security culture as the shared values and beliefs that people in an organization have about security. When implementing information security there is change. An important aspect is that organizations do not change, but people change and therefore people change organizations. To implement information security the organization's corporate culture plays a significant role. If the corporate culture is correct the organization will have good security. This implies that a security conscious corporate culture needs to be created in the organization.

2.3.5 External Factors

External factors are outside influences that can impact information security of an organization. Various external factors can impact the ability of a business or investment to achieve its strategic goals and objectives. Some of the external factors include strategic partners, government regulations, baseline standards, legislation and law and political environment.

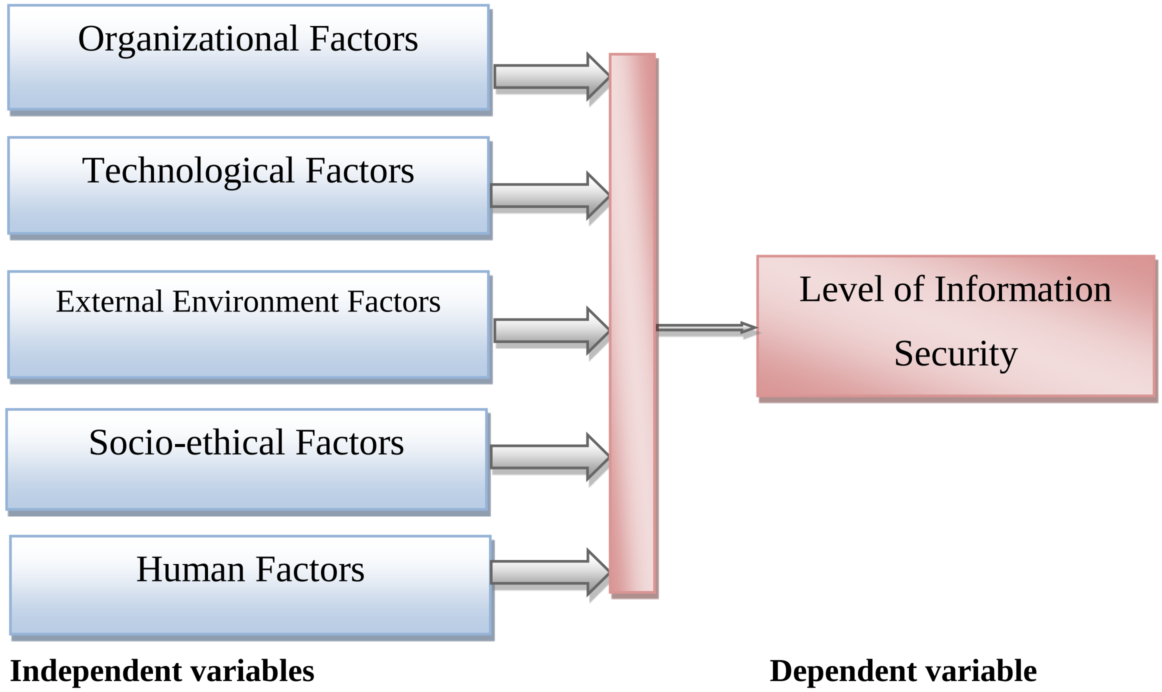
2.3.5.1 Baseline Standards - Organization are prone to several threats if appropriate measures are not in place and lack of a strong information system increases the cost of an organization while trying to manage information security in an unstructured manner. Standards and methods are used as reference for valuable resources for people dealing with Information Security. Codes of practice helps organization take information security seriously, as they give a wide range of security issues such as system policy, system organization compliance, and physical control system organization. International standards such as ISO 17799 help the organization in making sure that the most important concepts, which are internationally accepted by all organizations, are covered. They can serve as a guide for management to implement information security.

2.3.5.2 Legislation/Law - The organization needs to operate according to the specified regulations of the law and to incorporate this into the information security management process. Staffs also need to know what their rights are and the punishment to be meted out if they were to transgress or infringe upon other people's rights or organization requirements. Laws protect against all computer-misuse offences by protecting against unauthorized access to computer material; unauthorized access with intent to commit or facilitate commission of further offences and unauthorized modification of computer material.

2.4 Conceptual Framework

This section describes the conceptual framework. The conceptual framework illustrates the independent and dependent variables. The independent variables are technological factors, human related factors and organizational factors, socio-cultural factors and external environmental factors and are assumed to influence information security.

Figure 1: Conceptual Framework



Description of the proposed framework

i. Organization factors aspects are those related to the structure of the organization, including size and managerial decisions around information security and contain elements like management support, budget allocation, information security policy enforcement and adaptation, organization mission and risk analysis.

ii. Technological factors include complexity of systems, mobile and distributed access, vulnerability in systems and applications, and access controls

iii. Human factors which relate to cognition at the individual level, and interaction with other people include awareness, and information security training and education

iv. External environment factors which involves the interaction with the outside environment of an organization contain elements like strategic partners, government regulations, baseline standards, and legislation and law

v. Socio-cultural factors are set of beliefs, customs, practices and behavior that exists within a population, and include ethics, culture and religion

vi. Information security is the confidentiality, integrity, and availability of information.

2.5 Chapter Summary

The above chapter reviewed the various theories that explain the independent and dependent variables. The reviewed theories are then critiqued for relevance to specific variables. The chapter also explored the conceptualization of the independent and the dependent variables by analyzing the relationships between the two set of variables. In addition, an empirical review was conducted where past studies both global and local was reviewed in line with the following criteria, title, scope, methodology resulting into a critique. It is from these critiques that the research gap was identified.

CHAPTER THREE:

RESEARCH METHODOLOGY

3.0 Introduction

The main objective of this study was to propose a framework for improving the level of information security in public financing institutions in Kenya. This chapter describes the methodology and tools used to conduct the research study in order to validate our framework.

3.1. Research Design

The study employed descriptive research design utilizing a single case study approach. Descriptive research is also called statistical research. The main goal of this type of research is to describe the data and characteristics about what is being studied hence its adoption as the main objective was to evaluate factors affecting the level of information security levels in public financing institutions. The idea behind this type of research is to study frequencies, averages, and other statistical calculations. A survey is the analysis of more than one unit given a population. Descriptive survey study design is therefore appropriate because it is possible to obtain data from a cross section of Officers in Higher Education Loans Board (HELB).

3.2 Target Population

In a research study, population refers to those who can provide the required information (Peil, 1995). A population therefore entails all the cases or individuals that fit specifically for being sources of the data required addressing the research problem. The target population was the staff of HELB, who totaled 119 in number at the time of conducting the research.

3.3 Sample Size and sampling Technique

A simple approach to sample size calculation is to use the formula for calculating a sample size without putting into consideration the population and assuming a probability of 50/50. Mugenda and Mugenda (2003) further recommend the following formula for sample size determination;

$n = p(1-p)\left(\frac{z}{d}\right)^2$ Where:

n’= sample size

z= the table value for the level of confidence, for instance 95% level of confidence =1.96, 90% level of confidence =1.645.

d= margin of error

p= proportion to be estimated, Mugenda and Mugenda (2003) recommends that if you don’t know the value of p then you should assume p=0.5

Therefore, the sample size of this study was calculated as follows:

$$n = 0.5(1-0.5)\left(\frac{1.645}{0.10}\right)^2 = 68$$

Therefore a stratified random sampling technique was used and yielded the following respondents. To identify the actual respondents, a form of random sampling technique known as the lottery method was used. A proportion of 68/119 (34%) was used to arrive at the number of respondents in each department.

Table 3.1 Sample Size

Department	**Population**	**Sampling ratio**	**Sample size**
MIS services (Technical users)	12	34%	6.8
Loan disbursement and recoveries	55	34%	31.4
General administration (HR, finance, Audit Quality assurance)	52	34%	29.6
Total	**119**	**34%**	**68**

Source: HELB Human resource department records

3.3 Data Collection

In order to investigate factors affecting the level of information security in public financing institutions the study used the following methods to collect data.

3.3.1 Questionnaire

The study used primary data collected through a self-administered questionnaire. A questionnaire is a means of eliciting the feelings, beliefs, experiences, perceptions, or attitudes of some sample of individuals. The questionnaire is preferred because it is easier to administer, analyze and economical in terms of time and money. The questionnaire was developed based on the five factors affecting information security levels as reviewed in the literature. The questionnaire comprised closed ended questions. Each question was measured on a 5 point likert-type scale as follows. Data was analyzed using SPSS 11.5

1. Strongly Disagree
2. Disagree
3. Not sure
4. Agree
5. Strong agree

3.3.2 Interview

Interview technique was the second option used to gather primary data and is the best way to acquire deeper information from the population. Interviews were conducted to supplement questionnaire for the purpose of clarity on certain concepts that that did not come out clearly from the questionnaire

3.3.3 Review documents

Relevant documents were reviewed to give more light of the practices on information security in HELB

3.4 Pilot Test

The questionnaire was subjected to a review by experts in the area of information security who gave their contribution towards the content of the data collection tool. This was done to check the clarity of the concepts in the questionnaire. The questionnaire was then piloted on representative sample in order to assess the reliability and factorial validity of the test items. Six questionnaires were distributed among the members of staff two from each identified strata(identified departments) all the six questionnaires were received back fully filled The input from this discussion was added to the questionnaire before distributing the same to the respondents.

3.4.1 Validity

According to Cooper & Schindler (2007) validity is the extent to which a given finding depicts what it is believed to show. In order to confirm the validity of the research tool they are carefully examined to confirm proper coverage of the research objectives and ensure content validity. Patton (1990) refers to content validity as meaning that the instruments comprised a representative sample of all the possible items for each category area. The following measures were taken for validity

i. Data was collected from a reliable source
ii. Survey questions were based on the literature review
iii. Questionnaire was pretested for meaning and semantics by experts in information security

3.4.2 Reliability

Reliability is that quality of measurement method that suggests that the same data was collected each time in repeated observation of the same phenomenon, (Chandran, 2004). The reliability of the questionnaire was determined through a pilot study. According to Kothari (1990) 1 to 5% of sample size is adequate for pilot testing. The respondents for pilot test were 5 members of staff working at the HELB. Cronbach's coefficient Alpha formula was used to estimate the internal consistency of the study tool (Breakwell, 1995). The reliability coefficient of 0.7 and above was recommended (Cronchbach, 1951). Reliability results in table 3.2 indicate that the questionnaire was reliable.

Table 3. 1: Reliability Statistics for the pilot study

Cronbach's Alpha	N of Items	Number of Respondents
.914	30	5

3.5 Data Analysis

This research yielded quantitative data from the questionnaires, which were be analyzed using descriptive statistics and factor analysis. The descriptive statistics enabled the research study to offer meaningful description to the distribution of scores or measurements using a few indices or statistics (Cooper and Schilder, 2011). In particular, frequencies, mean scores, standard deviation, averages and percentages were used.

3.6 Data presentation

Data was presented using tables, pie chart and graphs. According to Kumar (2005), the main purpose of using data-display techniques is to make the findings clear and easily understood having analyzed the data. Tables are the most common method of presenting analyzed data, and they offer a useful means presenting large amounts of detailed information in a small space. In the study, both frequency tables and cross-tabulations were used. The main objective of a graph was to present data in a way that is easy to understand and interpret, and interesting to look at it (Kumar, 2005). Graphic presentations often make it easier to see the pertinent features of a set of data. In this research study Bar Charts for displaying categorical data, histogram and frequency polygons. These tools were selected because of their ease of understanding and clarity in presentation.

3.7 Develop a framework Model

The results and analysis of the questionnaire was the basis of the security improvement framework. The final outcome of all these activities is framework for security improvement.

3.8 Validating the Information Security model

The draft information security improvement framework was validated through the use of statistical regression analysis.

CHAPTER FOUR:

DATA PRESENTATION

4.0 Introduction

The purpose of data collection was to test the validity of information security framework. In this chapter presents the research findings and the interpretation from the data collected from case study organization (HELB). The findings will be presented using parametric statistical methods such as frequency tables, cross tabulations, and regression analysis. Out of the 68 questionnaires that were handed out, 60 (88.23%) questionnaires were returned fully filled. According to Mugenda and Mugenda (2003), a response rate of 50 % or more is ideal for data analysis.

4.1 Reliability Results

Reliability can be defined as the fact that a scale should consistently reflect the construct it measuring. Cronbach alpha coefficient was used to estimate the internal consistency and reliability on the data from the field. As indicated if table 4.1 A cronbach alpha of was realized 0.884 which exceeds 0.7 that is the lower limit of acceptability indicating that the questionnaire and the individual items included in the questionnaire were reliable.

Table 1: Reliability Statistics

Cronbach's Alpha	N of Items	Number of Respondents
.884	30	60

4.2 Demographic Characteristics

4.2.1 Gender of Respondents

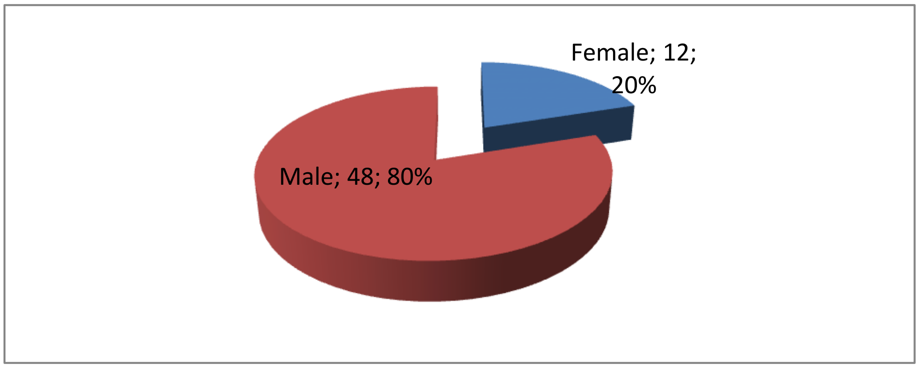


Figure 4.2.1 Gender response

According to figure 4.2.1, a majority (80%) of the respondents were male. Female respondents were 20% of the respondents.

4.2.2 Number of Years Worked

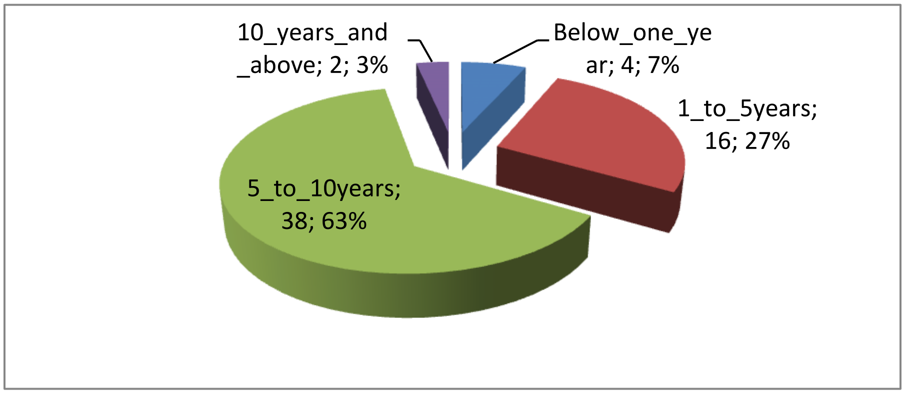


Figure 4.2.2 No. of years worked

Results in figure 4.2.2 revealed that the 63% of respondents indicated that they had worked at HELB for over 10 years. Results also indicated that 27% of respondents had worked at HELB for a period between 1 to 5 years. 7% of the respondents indicated that they had worked at HELB for a period below one year. Only 3% of respondents had worked at HELB for 10 years and above. The findings implied that most of the respondents had worked at HELB for a substantial period of time to be knowledgeable about information security.

4.2.3 Level of Education of the Respondents

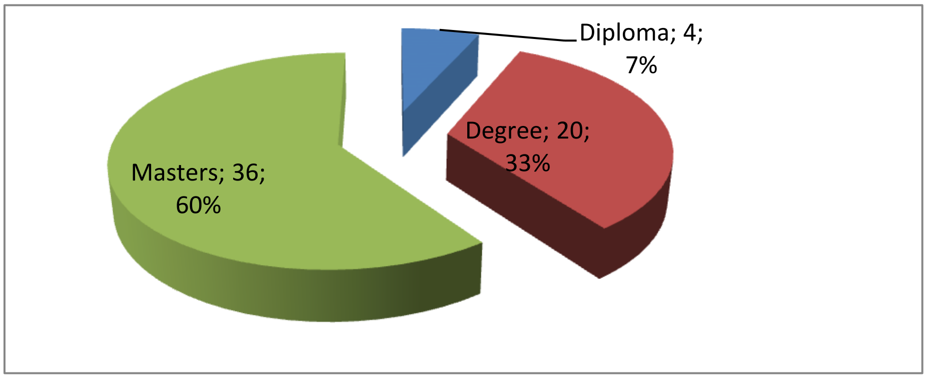


Figure 4.2.3 Level of education

Figure 4.2.3 reveals that 60% of respondents had Master's Degree as their highest level of education. Meanwhile, 33% had degree level of education followed by 7% who had diploma level of education. The findings imply that majority of the respondents were highly educated and this may have contributed to the accuracy and coherence of the study results.

4.2.4 Position of the Respondents

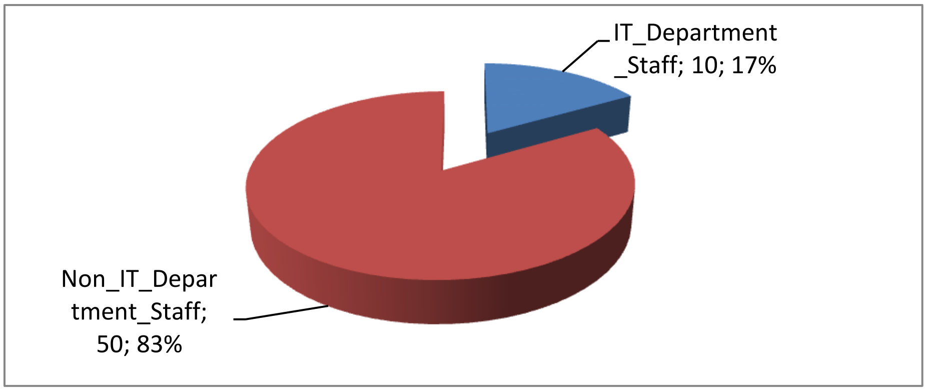


Figure 4.2.4 Position of the Respondents

Table 4.2.4 83% of respondents indicated that they were not in the IT Department. Meanwhile, 17% of the respondents indicated that they were in the IT Department.

4.2.5 Computer Knowledge

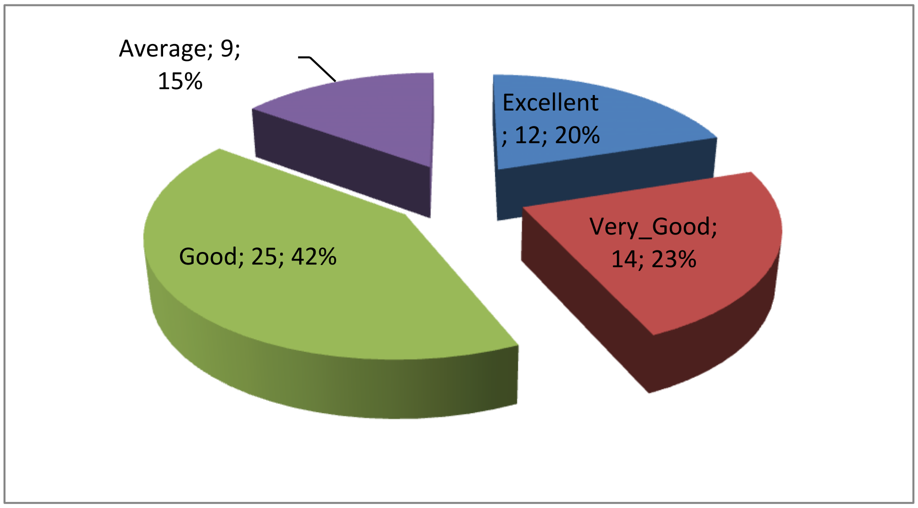


Figure 4.2.5 Computer Knowledge

Figure 4.2.5 reveals that 42% of respondents indicated that they understood computer quite well while 23% of the respondents indicated that their computer knowledge was very good. Meanwhile, 20% indicated that they were excellent in computer knowledge and finally 15% of the respondents indicated that they only had average knowledge in computer. The findings imply that majority of the respondents were computer literate and this may have contributed to the accuracy and coherence of the study results.

4.2.6 Understanding IS Security

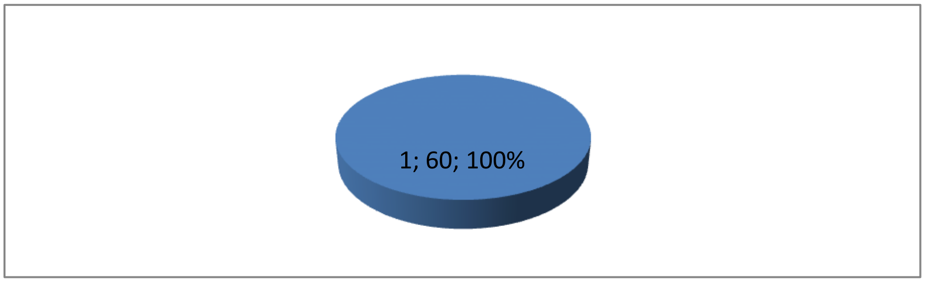


Figure 4.2.6 Understanding IS Security

Figure 4.2.6 reveals that there was a unanimous agreement among all the respondents whereby they all indicated that they understood IS Security.

4.3 Descriptive Results

Descriptive analysis was conducted in order to establish the level of IS security at HELB. The individual questions that represented the level of security were presented in this section.

4.3.1 Management support

The findings in Table 2 reveal that 65% of the respondents agreed with that they were aware that the management was giving its support to information security process in HELB while, 15% of the respondents disagreed with the statement that the management was giving its support to information security process in HELB and another 15% of the respondents neither agreed nor disagreed with the statement. However, 5% of the respondents strongly agreed with the statement thus summing up to 70% of those who agreed. 6 out 8 of the respondents from ICT department disagreed with the perception that management give support to information security process. Further enquiry through direct interview to establish why respondents believed that the management supported information security while the ICT department staffs think otherwise is that staff believed that it’s the responsibility of ICT department to prioritize their programs and manage information security while, the managements responsibility is to provide resources.

Table 2: Management support to information security process in HELB

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	0	0.0	0.0	0.0
	Disagree	9	15.0	15.0	15.0
	Not sure	9	15.0	15.0	30.0
	Agree	39	65.0	65.0	95.0
	Strongly Agree	3	5.0	5.0	100.0
	Total	60	100.0	100.0	

The findings in Table 3 reveal 30% of the respondents neither agreed nor disagreed with the statement that the management of HELB prioritizes information security. Meanwhile, 25 % of the respondents agreed with the statement that the management of HELB prioritizes information security and 10% of the respondents strongly agreed with the statement thus bring into a sum of 35% of those who agreed. Twenty percent (20) of the respondents however, disagreed with the statement and 15% strongly disagreed summing up to a total of 35% of those whole disagreed. This means the majority of the respondents do not believe the management prioritizes information security.

Table 3: Management of HELB prioritizes information security

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	9	15.0	15.0	15.0
	Disagree	12	20.0	20.0	35.0
	Not sure	18	30.0	30.0	65.0
	Agree	15	25.0	25.0	90.0
	Strongly Agree	6	10.0	10.0	100.0
	Total	60	100.0	100.0	

4.3.2 Budgetary allocation

The findings in Table 4 35% of the respondents neither agreed nor disagreed with the statement that Information security is part of the overall annual budget for HELB. Meanwhile, another equal majority of 35% of the respondents agreed with the statement that Information security is part of the overall annual budget for HELB. However, 15% of the respondents disagreed with the statement and finally another equal majority of 15% of the respondents strongly agreed with the statement that Information security is part of the overall annual budget for HELB therefore summing up to a total of 50% of those who were in agreement. A review of the budgetary allocation for the last two years does show budgetary allocation for software’s related to information security like firewall software’s, antivirus licenses, this showed the budget only took care of technical factors only.

Table 4: Information security is part of the overall annual budget for HELB

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	0	0.0	0.0	0.0
	Disagree	9	15.0	15.0	15.0
	Not sure	21	35.0	35.0	50.0
	Agree	21	35.0	35.0	85.0
	Strongly Agree	9	15.0	15.0	100.0
	Total	60	100.0	100.0	

The findings in Table 5 reveal that 55% of the respondents agreed with the statement that Information security is part of the ICT department budget. Meanwhile, 35% of the respondents neither agreed nor disagreed with the statement that Information security is part of the ICT department budget. However, 5% of the respondents strongly disagreed with the statement and finally, another 5% of the respondents disagreed with it thus bringing to a sum of 10% of those who disagreed.

Table 5: Information security is part of the ICT department budget

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	3	5.0	5.0	5.0
	Disagree	3	5.0	5.0	10.0
	Not Sure	21	35.0	35.0	45.0
	Agree	33	55.0	55.0	100.0
	Strongly Agree	0	0.0	0.0	100.0
	Total	60	100.0	100.0	

4.3.2 Information security policy

Results in table 6 reveal that 60% of respondents indicated that they were unsure about whether they were aware that HELB has a written information security policy. Meanwhile, a total of 30% disagreed with the statement while 10% agreed. The results imply that employees are not aware of any written information security policy. Further enquiries from the ICT department staff indicate there is no information security policy.

Table 6: Awareness that HELB has a written Information security policy

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	6	10.0	10.0	10.0
	Disagree	12	20.0	20.0	30.0
	Not Sure	36	60.0	60.0	90.0
	Agree	6	10.0	10.0	100.0
	Strongly Agree	0	0.0	0.0	100.0
	Total	60	100.0	100.0	

Results in table 7 reveal that 45% of respondents disagreed while another 25% strongly disagreed bringing to a total of 70% those who disagreed that they have access to HELB Information security policy. Meanwhile, 30% were unsure and a further 5% agreed with the statement. The results imply that employees do not have access to HELB information security policy. This further implies that there is a weakness in the level of IS security.

Table 7: Access to HELB Information security policy

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	15	25.0	25.0	25.0
	Disagree	27	45.0	45.0	70.0
	Not Sure	15	25.0	25.0	95.0
	Agree	0	0.0	0.0	95.0
	Strongly Agree	3	5.0	5.0	100.0
	Total	60	100.0	100.0	

4.3.4 Organization Mission

From the findings in Table 8 50% of the respondents neither agreed nor disagreed with the statement that HELB has allocated enough qualified staff for enhancing Information security. Meanwhile, 30% of the respondents agreed with the statement. Five percent (5%) of the respondents strongly agreed with the statement too thus summing up the total of those who agreed to 35%. However, 10% of the respondents disagreed with the statement and finally 5% of the strongly disagreed with it thus bringing the total of those who disagreed to 15%. There is no position of information officer within the ICT department implying everyone in the department handles security issue.

Table 8: HELB has allocated enough qualified staff for enhancing IS

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	3	5.0	5.0	5.0
	Disagree	6	10.0	10.0	15.0
	Unsure	30	50.0	50.0	65.0
	Agree	18	30.0	30.0	95.0
	Strongly Agree	3	5.0	5.0	100.0
	Total	60	100.0	100.0	

The findings in Table 9 shows 15% of the respondents disagreed with the statement that HELB has a security committee that reports it findings to the management and 10% strongly disagreed with it thus bringing to a total of 25% of those who disagreed. However, of 5% of the respondents agreed with the statement. From the ICT staff response there is no information security committee. Information Security is not just about information technology. Discussions about information security in any organization need to include more than just the technical team. A committee that blends information technology with information and business process owners is necessary to have the discussions needed to have to secure value. Many regulatory standards and best practice guidelines have some version of a security team in place because it is a best practice to have information security discussions at a business, not technical, level to know if the right choices for the business are made.

Table 9: HELB has a security committee that reports it findings to the management

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	6	10.0	10.0	10.0
	Disagree	9	15.0	15.0	25.0
	Not sure	42	70.0	70.0	95.0
	Agree	3	5.0	5.0	100.0
	Strongly Agree	0	0.0	0.0	100.0
	Total	60	100.0	100.0	

4.3.5 Risk Analysis

Findings in Table 10 55% of the respondents neither agreed nor disagreed with the statement that they were aware that HELB frequently evaluates the risks to its information systems. Meanwhile, 20% of the respondents agreed with the statement and 5% strongly agreed thus bringing to a total of 25% of those who agreed. However, 15% of the respondents disagreed with the statement and 5% of the respondents strongly disagreed with the statement thus bringing to a total of 20% of those who disagreed.

Table 10: HELB frequently evaluates the risks to its information systems

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	3	5.0	5.0	5.0
	Disagree	9	15.0	15.0	20.0
	Not sure	33	55.0	55.0	75.0
	Agree	12	20.0	20.0	95.0
	Strongly Agree	3	5.0	5.0	100.0
	Total	60	100.0	100.0	

The findings in Table 11 40% of the respondents neither agreed nor disagreed with the statement that they were aware that HELB has a specific team of individuals that are responsible for information security. On the other hand, 30% of the respondents agreed with the statement and 10% strongly agreed thus making a total of 40% of those who agreed. However, 15% of the respondents disagreed with the statement and 5% strongly disagreed making a total of 20% of those who disagreed. Further inquiry from staff why they believe there is a team revealed that they consider ICT department to be the team.

Table 11: HELB has specific individuals who are responsible for IS

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	3	5.0	5.0	5.0
	Disagree	9	15.0	15.0	20.0
	Not Sure	24	40.0	40.0	60.0
	Agree	18	30.0	30.0	90.0
	Strongly Agree	6	10.0	10.0	100.0
	Total	60	100.0	100.0	

The findings in Table 12 indicates 45% of the respondents not sure with the statement that risks are communicated to the people who are responsible for resolving the risks. 25% of the respondent disagreed with the statement and 5% strongly disagreed thus bringing into a total of 30% of those who disagreed. However, 20% of the respondents agreed with the statement and 5% strongly agreed thus totaling to 25% of those who agreed.

Table 12: Risks are communicated to the people responsible for resolving to resolve.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	3	5.0	5.0	5.0
	Disagree	15	25.0	25.0	30.0
	Not Sure	27	45.0	45.0	75.0
	Agree	12	20.0	20.0	95.0
	Strongly Agree	3	5.0	5.0	100.0
	Total	60	100.0	100.0	

4.3.6 Information security awareness

Table 13 shows that 35% of the respondents disagreed with the statement that there is appropriate awareness program at HELB staffs are aware of their security responsibility and a further 20% of the respondents strongly disagreed hence bringing to a total of 55% of those who disagreed with the statement. 20% of the respondents however, agreed with the statement and 10% strongly agreed totaling to 30% of those who agreed. Finally, 15% of the respondents neither agreed nor disagreed with the statement.

Table 13: Appropriate awareness program at HELB staff

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	12	20.0	20.0	20.0
	Disagree	21	35.0	35.0	55.0
	Not Sure	9	15.0	15.0	70.0
	Agree	12	20.0	20.0	90.0
	Strongly Agree	6	10.0	10.0	100.0
	Total	60	100.0	100.0	

The findings in Table 14 35% of the respondents disagreed with the statement that they were aware that information security awareness exercises are frequently undertaken by HELB. Besides, 10% of the respondents strongly disagreed with the statement thus making a total of 45% of those who disagreed. On the other hand 30% of the respondents neither agreed nor disagreed with the statement. However, 20% of the respondents agreed with the statement and 5% strongly agreed with it thus making a total of 25% of those who agreed.

Table 14: Information security awareness exercise are frequently undertaken.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	6	10.0	10.0	10.0
	Disagree	21	35.0	35.0	45.0
	Not Sure	18	30.0	30.0	75.0
	Agree	12	20.0	20.0	95.0
	Strongly Agree	3	5.0	5.0	100.0
	Total	60	100.0	100.0	

The above tables 13 and 14 indicate that HELB does not carry out any awareness program for its staff on information security.

4.3.7 Information security training

The findings in Table 15 45% of the respondents disagreed with the statement that HELB gives regular and structured training program to all members of staff on information security. Besides, 35% of the respondents strongly disagreed thus making a total of 80% of those who disagreed with the statement. However, 5 % of the respondents agreed with the statement while 15%.

Table 15: Regular and structured training program to members of staff on IS

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	21	35.0	35.0	35.0
	Disagree	27	45.0	45.0	80.0
	Not Sure	9	15.0	15.0	95.0
	Agree	3	5.0	5.0	100.0
	Strongly Agree	0	0.0	0.0	100.0
	Total	60	100.0	100.0	

The findings in Table 16 shows 45% of the respondents disagreed with the statement that HELB gives them specific training about information security procedures i.e. safekeeping of confidential documents that they must follow. Still in the same breath, 40% of the respondents strongly disagreed with the statement thus summing up to a total of 85% of those who disagreed. However, 15% of the respondents indicated that they were unsure. No training on information security from the above two questions.

Table 16: HELB gives me specific training about information security procedures

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	24	40.0	40.0	40.0
	Disagree	27	45.0	45.0	85.0
	Not Sure	9	15.0	15.0	100.0
	Agree	0	0.0	0.0	100.0
	Strongly Agree	0	0,0	0.0	100.0
	Total	60	100.0	100.0	

4.3.8 Legislation and law

The findings in Table 17 45% of the respondents agreed with the statement that they are aware of the legal implications of information they have access to. In the same line, 10% of the respondents strongly agreed with the statement thus bringing to a total of 55% of those who agreed. However, 30% of the respondents strongly disagreed and 10% disagreed hence making a total of 40% of those who disagreed. 5% of the respondents neither agreed nor disagreed with the statement.

Table 17: I am aware of the legal implications of information I have access to

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	18	30.0	30.0	30.0
	Disagree	6	10.0	10.0	40.0
	Not Sure	3	5.0	5.0	45.0
	Agree	27	45.0	45.0	90.0
	Strongly Agree	6	10.0	10.0	100.0
	Total	60	100.0	100.0	

4.3.9 Baseline standards

The findings in Table 18 shows 70% of the respondents are not sure with the statement that HELB is certified by any international security standards like COBIT, ITIL. On the other hand 15% of the respondents disagreed with the statement and 10% strongly disagreed thus making a total of 25% of those who disagreed. Five percent (5%) however, strongly agreed with the statement. All the ICT staff who respondent to the questionnaire disagreed with the statement that HELB is certified by any international security standard.

Table 18: HELB certified by international security standards like COBIT, ITIL

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	6	10.0	10.0	10.0
	Disagree	9	15.0	15.0	25.0
	Not Sure	42	70.0	70.0	95.0
	Agree	0	0.0	0.0	95.0
	Strongly Agree	3	5.0	5.0	100.0
	Total	60	100.0	100.0	

The findings in Table 19 indicate 65% of the respondents not sure that HELB employs international accepted standards like COBIT, COSO, and ITL to manage information. Meanwhile, an equal percentage of 10% disagreed and strongly disagreed with the statement respectively thus bringing to a total of 20% of those who disagreed. However, 10% of the respondents strongly agreed with the statement and 5% agreed with it thus making a total of 15% of those who agreed. Again ICT staff who responded disagreed with the statement that HELB employs any internationally accepted standard to manage information security

Table 19: HELB employs international standards to manage information security

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	6	10.0	10.0	10.0
	Disagree	6	10.0	10.0	20.0
	Not Sure	39	65.0	65.0	85.0
	Agree	3	5.0	5.0	90.0
	Strongly Agree	6	10.0	10.0	100.0
	Total	60	100.0	100.0	

Internationally accepted standards such as ISO 17799, COBIT do serve as a guide for the organization and ensuring that the most important concepts, which are internationally accepted by all organizations, are covered.

4.3.10 Socio-ethical awareness

The findings in Table 20 55% of the respondents agreed with the statement that they were aware that the work they were doing was part of HELB property. In the same line, 45% of the respondents strongly agreed with the statement too thus all the respondents agreed with the statement. This means that the right of an individual and an organization to ownership of all information about them or of all information that has been gathered at their expense are protected, for instance all the codes belong to HELB and cannot be sold by an employee as there are procedures to protect them.

Table 20: The work I do is part of HELB property

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	0	0.0	0.0	0.0
	Disagree	0	0.0	0.0	0.0
	Not Sure	0	0.0	0.0	0.0
	Agree	33	55.0	55.0	55.0
	Strongly Agree	27	45.0	45.0	100.0
	Total	60	100.0	100.0	

The findings in Table 21 45% of the respondents agreed with the statement that they were aware that the management considers their personal information as private. However, 40% of the respondents neither agreed nor disagreed with the statement. Meanwhile, 5% percent of the respondents strongly agreed with the statement thus bringing to a total of 50% of those who agreed. Finally, 10% of the respondents disagreed with statement. Quite a substantial portion of the respondents neither agree or disagree implying the have not been put through the process that shows how HELB respects their privacy,

Table 21: The management considers my personal information as private

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	0	0.0	0.0	0.0
	Disagree	6	10.0	10.0	10.0
	Not Sure	24	40.0	40.0	50.0
	Agree	27	45.0	45.0	95.0
	Strongly Agree	3	5.0	5.0	100.0
	Total	60	100.0	100.0	

4.3.11 Information security culture

The findings in Table 22 show 35% of the respondents strongly agreed with the statement that they consider Information security as a technical issue and therefore should be handled by ICT staff further, 30% of the respondents agreed with statement thus totaling to 75% of those who agreed. On the other hand, 28% of the respondents disagreed with the statement and 7% of the respondents strongly disagreed making a total of 35% of those who disagreed.

Table 22: I consider IS a technical issue and therefore should be handled by ICT staff

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	4	6.7	6.7	6.7
	Disagree	17	28.3	28.3	35.0
	Not Sure	0	0.0	0.0	35.0
	Agree	18	30.0	30.0	65.0
	Strongly Agree	21	35.0	35.0	100.0
	Total	60	100.0	100.0	

The findings in Table 23 indicate 50% of the respondents agreed with the statement that they do open all the emails addressed to them even if they did not know the source. Meanwhile, 30% of the respondents strongly disagreed with the statement and 15% disagreed with it too thus making a total of 45% of those who disagreed. However, a simple majority of 5% agreed with the statement thus bringing to a total of 55% of those who agreed.

Table 23: I do open all the emails addressed to me even if I do not know the source

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	18	30.0	30.0	30.0
	Disagree	9	15.0	15.0	45.0
	Not Sure	0	0.0	0.0	45.0
	Agree	30	50.0	50.0	95.0
	Strongly Agree	3	5.0	5.0	100.0
	Total	60	100.0	100.0	

The findings in Table 24 shows 50% of the respondents strongly disagreed with the statement that due to their nature of work at times they share their password but they do change it. Meanwhile, 10% of the respondents disagreed with the statement too making a total of 60% of those who disagreed. However, 40% of the respondents agreed with the statement.

Table 24: Due to my nature of work at times I share my password but do change it

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	30	50.0	50.0	50.0
	Disagree	6	10.0	10.0	60.0
	Not Sure	0	0.0	0.0	60.0
	Agree	24	40.0	40.0	100.0
	Strongly Agree	0	0.0	0.0	100.0
	Total	60	100.0	100.0	

The findings in Table 25 52% of the respondents agreed with the statement that they had limited ability to download applications and install in their office desktop machine. Meanwhile, 18% strongly agreed making a total of 70% of those who agreed. However, 25% of the respondents disagreed while 5% neither agreed nor disagreed. The staff are able to install downloads in the office machines increasing the risks as some of this downloaded software's are sources of viruses and malware's

Table 25: Limited ability to download applications and install in desktop machine

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	0	0.0	0.0	0.0
	Disagree	15	25.0	25.0	25.0
	Not Sure	3	5.0	5.0	30.0
	Agree	31	51.7	51.7	81.7
	Strongly Agree	11	18.3	18.3	100.0
	Total	60	100.0	100.0	

4.3.12 Technological factors

The findings in Table 26 indicate that 65% of the respondents strongly agreed with the statement that HELB uses anti-virus to protect its IT systems further, 25% of the respondents agreed with the statement hence making a total of 90% of those who agreed. However, 5% of the respondents neither agreed nor disagreed and finally another 5% of the respondents disagreed with the statement.

Table 26: HELB uses anti-virus to protect its IT systems

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	0	0.0	0.0	0.0
	Disagree	3	5.0	5.0	5.0
	Not Sure	3	5.0	5.0	10.0
	Agree	15	25.0	25.0	35.0
	Strongly Agree	39	65.0	65.0	100.0
	Total	60	100.0	100.0	

The findings in Table 27 45% of the respondents strongly agreed with the statement that they were aware that HELB has a firewall. Besides, 40% of the respondents agreed with the statement thus bringing to a total of 85% of those who agreed. However, 15% of the respondents neither agreed nor disagreed with the statement.

Table 27: HELB has a firewall

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	0	0.0	0.0	0.0
	Disagree	0	0.0	0.0	0.0
	Not Sure	9	15.0	15.0	15.0
	Agree	24	40.0	40.0	55.0
	Strongly Agree	27	45.0	45.0	100.0
	Total	60	100.0	100.0	

The findings in Table 28 55% of the respondents strongly agreed with the statement that they were frequently made to change their password automatically and 40% agreed with the statement too making 95% of those who agreed. However, 5% of the respondents disagreed with the statement.

Table 28: I am frequently made to change my password automatically

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	0	0.0	0,0	0.0
	Disagree	3	5.0	5.0	5.0
	Not Sure	0	0.0	0.0	5.0
	Agree	24	40.0	40.0	45.0
	Strongly Agree	33	55.0	55.0	100.0
	Total	60	100.0	100.0	

4.3.13 information security (CIA)

The findings in Table 29 shows 65% of the respondents not sure with the statement that HELB information and system resources cannot be leaked out to unauthorized person easily, 5% agree while 5% strongly agree. Meanwhile, 20% strongly agreed and 5% agree. Only 25% are sure that information cannot be leaked out. This means it's possible to get information easily from HELB.

Table 29: Information and system resources cannot be leaked out

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	12	20.0	20.0	20.0
	Disagree	3	5.0	5.0	25.0
	Not Sure	39	65.0	65.0	90.0
	Agree	3	5.0	5.0	95.0
	Strongly Agree	3	5.0	5.0	100.0
	Total	60	100.0	100.0	

The findings in Table 30 35% of the respondents agreed with the statement that they were aware that HELB information and system resources cannot be altered by unauthorized persons and 10% of the respondents strongly agreed. Meanwhile, 25% of the respondents neither agreed nor disagreed with the statement, 15% each disagreed and strongly disagreed with the statement. Only 45% believe that information cannot be altered by unauthorized person this mean there chances of inconsistency in the information held by HELB

Table 30: Information and system resources cannot be altered

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	9	15.0	15.0	15.0
	Disagree	9	15.0	15.0	30.0
	Not Sure	15	25.0	25.0	55.0
	Agree	21	35.0	35.0	90.0
	Strongly Agree	6	10.0	10.0	100.0
	Total	60	100.0	100.0	

The findings in Table 31 shows 50% of the respondents agreed with the statement that they are able to account for all the HELB information they had shared with other organizations and customers further, 10% strongly agreed with the statement making a total of 60% of those who agreed. However, 20% of the respondents disagreed with the statement and 10% strongly disagreed making a total of 30% of those who disagreed. Finally, 10% of the respondents neither agreed nor disagreed with the statement. The small percentage who cannot account for the information they share with other persons or institutions is enough to subject HELB to legal battles as there should procedures of sharing information between HELB and clients

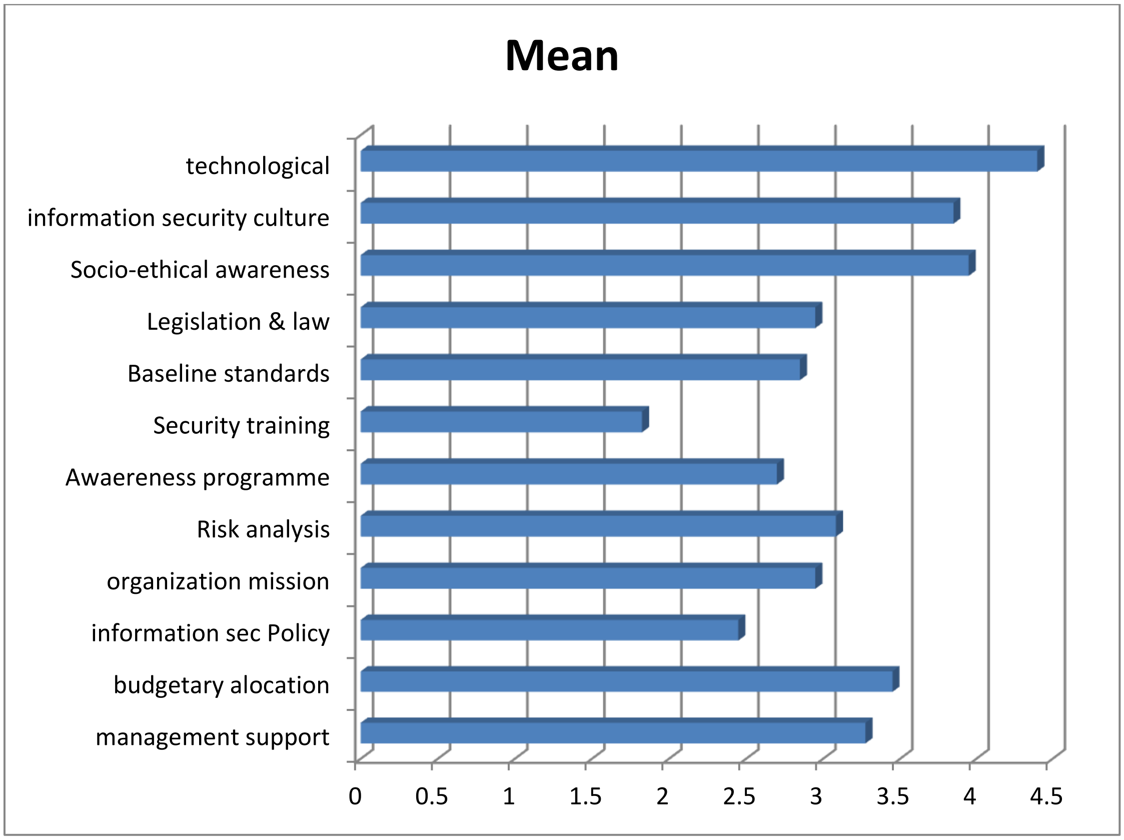
Table 31: Ability to account for all information I have shared

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	6	10.0	10.0	10.0
	Disagree	12	20.0	20.0	30.0
	Not Sure	6	10.0	10.0	40.0
	Agree	30	50.0	50.0	90.0
	Strongly Agree	6	10.0	10.0	100.0
	Total	60	100.0	100.0	

4.4 Evaluating the level of information security

The following graph 4.1 highlights the observation based on the results of questionnaire showing the areas of strength and weakness calculated by assigning one to a weakness five to strength. From the graph areas of weakness include security training, information security policy, awareness program, baseline standards, organization mission, legislation and laws as well as risk analysis processes. Areas of strength are technical, information security culture and socio-ethical awareness. This is a simple way institution can frequently evaluate the level of information security.

Graph 4.1 weighted mean of the factors



4.5 Factor Analysis

Factor analysis was conducted in order to reduce the 30 statements into a set of underlying factors. Communality indicates the extent to which a variable (statement) can be explained by the factors. The communalities presented in table 32 show how the 30 statements shared a significantly large variance

Table 32: Communalities

Communalities	Initial	Extraction
Management gives its support to IS process in HELB	1.000	.860
Management of HELB prioritizes IS	1.000	.934
IS part of the overall annual budget for HELB	1.000	.908
IS part of the ICT department budget	1.000	.286
HELB has a written IS policy	1.000	.805
Access to the HELB IS policy	1.000	.717
Enough qualified staff for enhancing IS	1.000	.905
HELB has an IS committee	1.000	.817
HELB frequently evaluates the risks	1.000	.912
HELB has specific team responsible for IS	1.000	.917
Risks are communicated	1.000	.915
Appropriate awareness program at HELB	1.000	.871
Frequent IS awareness program at HELB	1.000	.923
Regular and structured training program on IS	1.000	.932
Specific training about IS procedures	1.000	.904
Legal implications of information accessed	1.000	.771
HELB is certified by international security standards	1.000	.901
HELB employs international accepted standards	1.000	.913
The work I do is part of HELB property	1.000	.837
Management considers personal information as private	1.000	.877
Consider IS a technical issue	1.000	.888
Open all the emails without verifying source	1.000	.947
Share password	1.000	.863
Download applications and install	1.000	.828
HELB uses anti-virus	1.000	.874
HELB has a firewall system	1.000	.889
Frequently change password automatically	1.000	.810
HELB information and system resources cannot be leaked out	1.000	.810
HELB information and system resources cannot be altered	1.000	.940
account for all the HELB information shared	1.000	.935

Extraction Method: Principal Component Analysis.

From table 32 for instance, the communality of 0.860 for statement management 1l is the sum of the squared factor loadings, that is 0.886^2+0.063^2+0.210^2+0.073^2+0.147^2. All statements/variables had a high communality with factors with the exception of budgeting 2. The shared variance was only 0.286.

4.6 Factorial Extraction

The table 33 below list the eigenvalues associated with each linear component (factor) before extraction, after extraction and after rotation. Before extraction there are 30 linear components since there should as many eigenvalues as there are variables. The eigenvalue associated with each factor represent the variance explained by that particular linear component. For example factor 1 explains 32.828 of the total variance. All the factors with eigenvalue greater than 1 are displayed which leave 5 factors. The eigenvalues associated with these factors are displayed in the column labeled extraction sums of square loadings. The values in this part of the table are the same as the values before extraction, except that the values for the discarded factors are ignored, hence the blank table after the fifth factor. The last column labeled sum of squared loadings shows the eigenvalues after rotation.

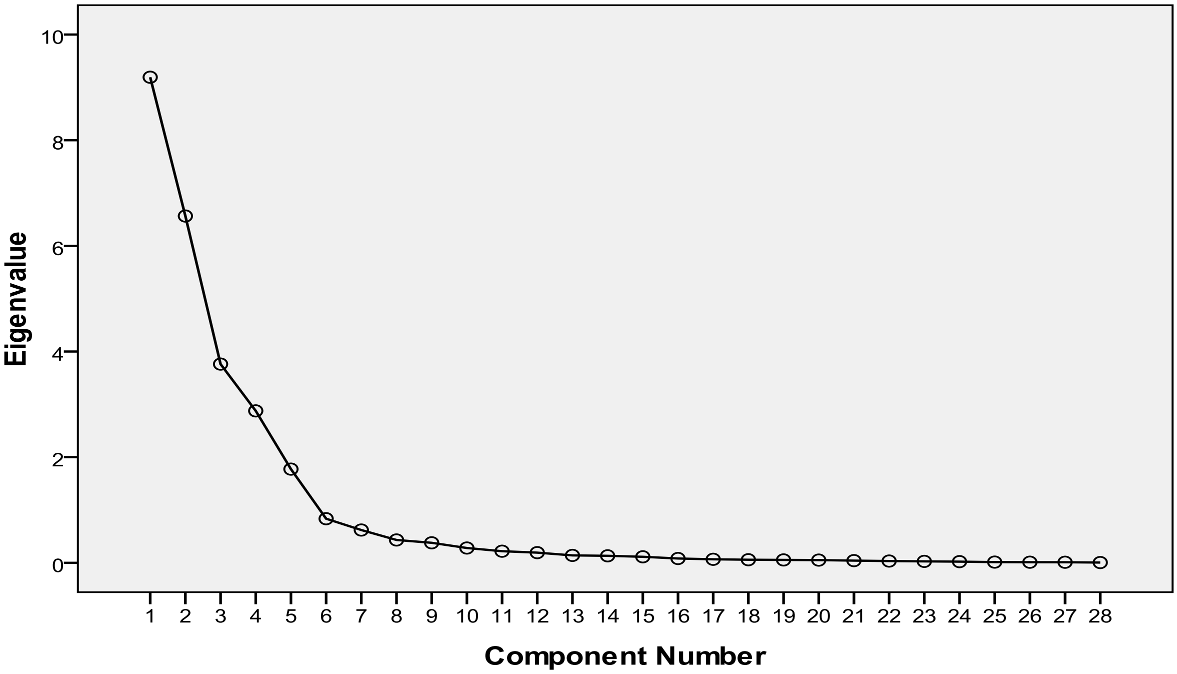
Factor analysis has extracted five factors according to Kaiser’s criterion which has been applied on the extraction by SPSS. Factor analysis is an exploratory tool and is only used as a guide to the number of factors to extract.

Table 33: Total variance explained of field data

	Initial Eigenvalues			Extraction Sums of Squared Loadings			Rotation Sums of Squared Loadings		
Component	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	9.192	32.828	32.828	9.192	32.828	32.828	7.268	25.956	25.956
2	6.565	23.445	56.274	6.565	23.445	56.274	5.258	18.780	44.736
3	3.762	13.435	69.709	3.762	13.435	69.709	5.228	18.671	63.407
4	2.876	10.273	79.982	2.876	10.273	79.982	3.876	13.843	77.250
5	1.774	6.334	86.316	1.774	6.334	86.316	2.538	9.066	86.316
6	.835	2.983	89.299						
7	.621	2.218	91.517						
8	.433	1.546	93.062						
9	.379	1.354	94.416						
10	.281	1.002	95.418						
11	.220	.786	96.204						
12	.193	.689	96.893						
13	.141	.502	97.395						
14	.133	.474	97.870						
15	.114	.408	98.278						
16	.082	.293	98.571						
17	.067	.239	98.809						
18	.059	.210	99.019						
19	.055	.197	99.216						
20	.052	.185	99.401						
21	.042	.149	99.550						
22	.034	.121	99.672						
23	.028	.098	99.770						
24	.022	.080	99.850						
25	.014	.050	99.899						
26	.012	.042	99.941						
27	.011	.040	99.981						
28	.011	.040	99.981						
29	.011	.040	99.981						
30	.005	.019	100.000						

Extraction Method: Principal Component Analysis.

Graph 4.2: Scree Plot for determining the number of factors



A scree plot presented in graph 4.2 indicated that factors affecting IS security can be reduced to a five factor model as shown from table 33

The rotated factor loadings

Table 34 shows that the statements in the first column shows the 10 statements weigh heavily on factor one relating to organization and management; these can therefore be grouped under organizational factors. Factor loadings of the next column shows the 6 statements weigh heavily on factor 2, these statements are associated with technology and access control. Factor loadings for third column show the six statements weighed heavily on factor 3 these six statements are associated with Social ethical and cultural factors. Column four statements weigh heavily on factor 4 these statements are associated with human resource and awareness training. The last column of the factor loadings shows 3 statements weighed heavily on factor 5 these 3 statements are associated with external environmental factors. These findings imply that the factors that affect IS security can be reduced to a five factor model

Table 34: Rotated component matrix on field data

	Component				
	1	2	3	4	5
management2	.958	.027	.116	.015	.030
Risk_analysis2	.941	.061	.109	.017	.127
Budgeting1	.941	-.092	.052	-.074	.077
Risk_analysis3	.936	.085	.134	.112	.020
Organizationmission1	.930	.098	.071	.046	.154
Risk_analysis1	.925	.125	.086	.139	.118
management1	.886	.063	.210	.073	.147
Organizationmission2	.856	.097	.166	.101	.193
Info_security_policy1	.840	.082	.266	.121	.113
Info_security_policy2	.832	.011	.166	.101	.193
Access_control2	.070	.939	-.230	.030	-.016
Access_control3	.087	.938	-.158	.094	-.116
Technological_factors1	.090	.918	-.012	.061	-.144
Technological_factors2	.003	.906	-.245	-.087	.038
Technological_factors3	-.034	.894	-.072	-.039	-.053
Access_control1	.185	.852	-.102	.184	-.078
Info_security_culture1	.137	-.134	.914	.080	.098
Info_security_culture2	.044	-.346	.901	.049	.106
Info_security_culture3	.129	-.072	.897	-.050	.182
Social_ethical_awareness1	.114	-.095	.883	-.055	.181
Social_ethical_awareness2	.191	-.141	.862	.083	.265
Info_security_culture4	.221	-.103	.856	.185	-.025
Awareness2	.102	.011	.040	.949	.101
Informationsecuritytraining2	.078	-.012	.053	.944	-.053
Informationsecuritytraining1	.163	.068	.122	.939	.055
Awareness1	.113	.031	.111	.914	.098
Budgeting2	.265	-.130	.118	-.409	.133
Baseline2	.281	-.060	.159	-.099	.892
Baseline1	.209	-.114	.199	.109	.890
Legislation_ and_law1	.154	-.169	.353	.098	.765

Figure 4.1 gives graphical model of the factorial loading

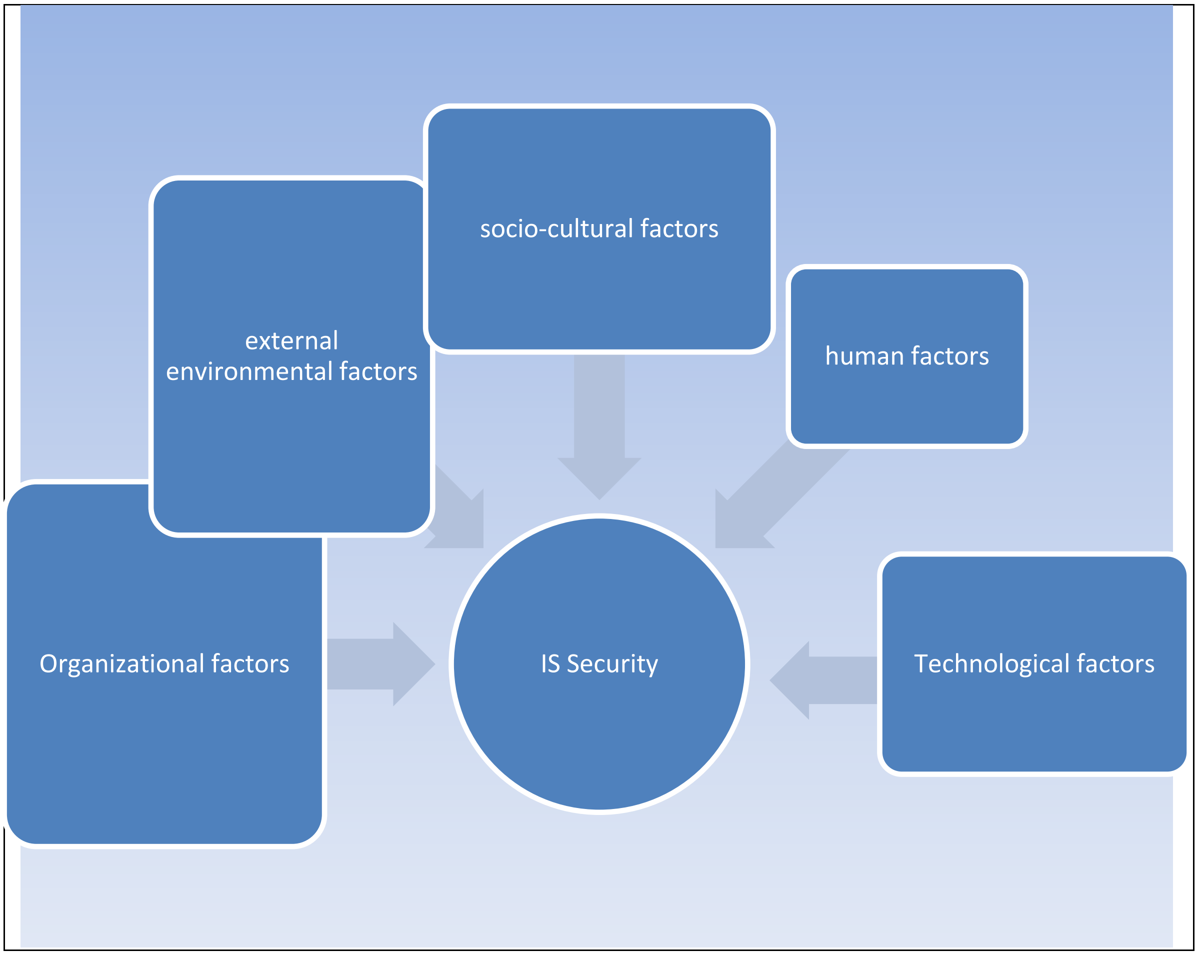


Figure 4.1: Model from factor loading

4.7 Model Validation Using Regression

Regression analysis is a statistical technique for estimating the relationships among variables. It includes many techniques for modeling and analyzing several variables, like the relationship between a dependent variable and one or more independent variables. More specifically, regression analysis helps one understand how the typical value of the dependent variable changes when any one of the independent variables is varied, while the other independent variables are held fixed. Therefore a regression analysis was conducted in order to validate the model of factors derived from factor analysis.

Table 4. 1: Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.904[a]	.818	.801	.49489

Predictors: (Constant), Socio-Cultural Factors, Human Factors, Technological Factors, Organization Factors, External Environmental Factors

Dependent Variable: Information Security

Results in table 4.35 indicate that an r squared of 0.818 was obtained. This implies that 81.8% of the variances in Information Security are explained by the five factors. This also implies that 18.2% of the variances in Information Security are explained by factors not included in the model.

Table 4. 2: Overall Model Significance (ANOVA)

Model		Sum of Squares	Df	Mean Square	F	Sig.
1	Regression	59.374	5	11.875	48.485	.000[a]
	Residual	13.226	54	.245		
	Total	72.600	59			

Predictors: (Constant), Socio-Cultural Factors, Human Factors, Technological Factors, Organization Factors, External Environmental Factors
Dependent Variable: Information Security

The result in table 4.36 indicate Anova statistic of 48.485 (p value=0.000) this indicates that the overall model was significant.

In an effort to investigate factors influencing information security i.e. socio-cultural factors, human factors, technological factors, organization factors, external environmental factors a multiple regression analysis was executed between the factors and information security. The results are displayed in table 4.3.

Table 4.3: Regression Coefficients

Model		Unstandardized Coefficients		Standardized Coefficients	T	Sig.
		B	Std. Error	Beta		
1	(Constant)	-3.074	.562		-5.471	.000
	Organization Factors	.130	.082	.101	3.582	.011
	Human Factors	.123	.071	.103	2.729	.009
	Technological Factors	1.325	.097	.851	13.705	.000
	External Environment Factors	.020	.075	.018	2.265	.007
	Socio-Cultural Factors	.111	.074	.101	3.494	.014

a. Dependent Variable: Information Security

Ho1: Organizational factors do not influence the level of Information security at HELB

The results in table 4.3 indicates that there is a positive and significant relationship between organization factors and Information security (b=0.13, t=3.582; p value=0.011). The pvalue is less that the benchmark/critical p value of 0.05. Hence, the null hypothesis of “no significant influence/no relationship” is rejected and the alternative “there exists a significant influence/ relationship” .This implies that an increase in management support and other attributes of organization by one unit leads to an increase in IS security by 0.13 units. The findings agree with those in (Doherty & Fulford 2005) who noted that without a proper budget, organizations won’t be equipped with sufficient resources to ensure information security. Organizations require adequate funding to achieve effective information security. The findings also agree with those in (Dinnie 1999) who noted that lack of information security budgeting in organizations leads to under- investment in appropriate controls. The findings also agree with those in Canavan (2003) who noted that there are essential operating systems, applications and other technologies which are required to support the implementation of information security in the organization. The findings also agree with those in Ciborra (2006) who argued that risk management emerged from people in organizations having a lack of knowledge, from the role of biased data when assessing risk in organizations and from the influence of internal politics. The findings also agree with those in Levine (2004) and Hughes (2006) who added that lack of clarity of the roles and responsibilities of people impacted on successful risk management. The findings also agree with those in Straub and Welke, (1998) who argued that organizations needs senior management support in order to gain a thorough understanding of organizational vulnerability and of the resources required in securing organizational systems. It is necessary that senior management understand the security actions required and for them to integrate security planning into information security policy through adoption of organizational standards, and that users are trained and educated about security awareness in order that organizational standards can be reviewed and updated.

Ho2: Human factors do not influence the level of Information security at HELB

The results in table 4.3 indicates that there is a positive and significant relationship between Human factors and Information security (b=0.123, t=2.729; p value=0.009). The pvalue is less that the benchmark/critical p value of 0.05. Hence, the null hypothesis of "no significant influence/no relationship" is rejected and the alternative "there exists a significant influence/ relationship". This implies that an increase in Human factors by one unit leads to an increase in IS security by 0.123 units. The findings agree with those in Hughes (2006) who noted that staff at all levels can help reduce risks; therefore, training programs, clarification of roles and responsibilities, and the identification of specific authority for specific roles must be provided for all staff to ensure success risk management. Lack of security awareness and training is perhaps the most concerning and often overlooked issue, with serious implications on ICT infrastructures. Likewise, training is another pungent issue amongst network administrators and technical staff that are in charge of ICT infrastructure and security. Because of a variety of factors, including lack of funding, awareness or support from top management, these people lack training and often fail to deal adequately with security issues.

Ho3: Technological factors do not influence the level of Information security at HELB

The results in table 4.3 indicates that there is a positive and significant relationship between technological factors and Information security (b=1.325, t=13.705; p value=0.000). The pvalue is less that the benchmark/critical p value of 0.05. Hence, the null hypothesis of "no significant influence/no relationship" is rejected and the alternative "there exists a significant influence/ relationship". This implies that an increase in technological attributes by one unit leads to an increase in IS security by 1.325 units. The findings agree with those in Schneier (2004) who need that in the last twenty years society has witnessed the flourishing of a myriad of electronic attacks, malware, vulnerabilities and intrusions in the domain of information and communication technologies and this is mainly due to the availability of attacking tools, automation and action at distance It is worth mentioning also that ICT security issues are not encountered only in the cyber space, but their impact is more noticeable and considerable in this domain.

Ho4: External environmental factors do not influence the level of Information security at HELB

The results in table 4.3 indicates that there is a positive and significant relationship between external environmental factors and Information security (b=0.02, t=2.265; p value=0.007). The pvalue is less that the benchmark/critical p value of 0.05. Hence, the null hypothesis of "no significant influence/no relationship" is rejected and the alternative "there exists a significant influence/ relationship". This implies that an increase in external environmental attributes by one unit leads to an increase in IS security by 0.02 units. The findings agree with those in Rashid (2001) who note that environmental factors provide significant impetus for adoption of ICT security measures where the issues relating to market climate and the firm's standing in the market directly influence the uptake of technology.

Ho5: Socio-cultural factors do not influence the level of Information security at HELB

The results in table 4.3 indicates that there is a positive and significant relationship between socio-cultural factors and Information security (b=0.111, t=3.494; p value=0.014). The pvalue is less that the benchmark/critical p value of 0.05. Hence, the null hypothesis of "no significant influence/no relationship" is rejected and the alternative "there exists a significant influence/ relationship". This implies that an increase in socio-cultural factors attributes by one unit leads to an increase in IS security by 0.111 units. The findings agree with those in Khaled (2003), Gakunu (2004), Aineruhanga (2004), Heeks (2003a), Ndou (2004), Bhatnagar (2003), Saul and Zulu (1994) who urged that Leadership styles, culture, and bureaucracy are inhibitors to information security.

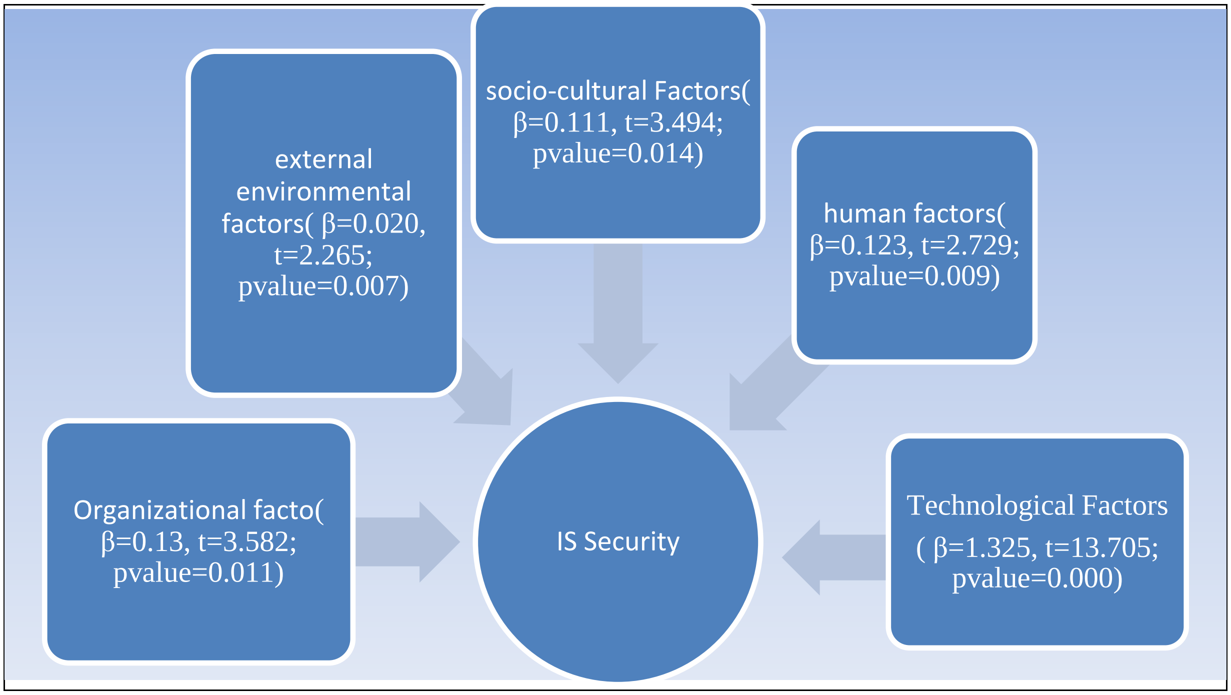

socio-cultural Factors(β=0.111, t=3.494; pvalue=0.014)
external environmental factors(β=0.020, t=2.265; pvalue=0.007)
human factors(β=0.123, t=2.729; pvalue=0.009)
Organizational facto(β=0.13, t=3.582; pvalue=0.011)
IS Security
Technological Factors (β=1.325, t=13.705; pvalue=0.000)

Figure 4.2: Final Validated Model

Results in figure 4.2 graphical indicated that the identified five factors are significantly influence the level of information security at HELB.

CHAPTER FIVE:

SUMMARY, CONCLUSION AND RECOMMENDATIONS

5.0. Introduction

The chapter addresses the research findings, conclusions and recommendations as well as limitations of the study and suggested areas of further studies. This was done in line with the objectives of the study.

5.1. Summary of Findings

In summary the main objective of this research project is to develop and validate a framework for the improvement of Information security levels in public financing institutions in Kenya. With other objectives being to determining the factors that influence the level of information security and to determine the level information security in public financing institutions case of Higher Education Loans Board (HELB).

5.1.1 Factors that influence the level of information security

Factors that influence the level of information security was one of the objectives of this study, and from the response of the staff that took part in the study found out the following facts about information security at HELB

- Management of information security is left to ICT department staff
- There is a reasonable budgetary allocation towards ICT department yet there is no specific allocation to Information security process.
- HELB does not have an information security policy in place
- HELB is most probably not having a security committee that report its findings to the management hence the management might not be fully aware of what exactly takes place as far as information security is concerned.
- There is no awareness campaigns on information security as well as information security training
- Information security risks are not evaluated
- HELB’s management of information security not aligned any baseline standards

- HELB has put in place adequate measures in terms of technical methods such as anti-viruses, firewalls and password managements

5.1.2 Levels of Information Security in Public Financing Institutions (HELB)

The other objective of the study was to determine levels of information security in public financing institutions a case of HELB. The results indicate that despite the fact that HELB has implemented information security enforcement strategies to a certain level mainly through technical methods as highlighted on graph 4.1 there are weaknesses areas like organizational, socio-cultural, human and external environment factors, this is also shown from the answers from the respondents stating either they are not sure or mostly disagreed with the statements relating to information security policy, organization mission, risk analysis, information security awareness programs, information security training, baseline standards, and information security culture.

5.1.3 The proposed/validated framework

A detailed analysis of factors influencing the level of information security gave the study insights on issues that need be addressed to make information security a success in organizations. By identifying the gaps and strengths the study gave the proposed framework as highlighted within the empirical study section. The purpose for going to collect data was to test the reliability and validity of our framework in chapter 4 and in chapter 5 the study provides information obtained from the field that validated the components of the framework.

5.2 Conclusions

The main objectives of the study was to come up with a framework for the improvement of information security levels in public financing institutions in Kenya by examining the factors that affect the level of information security at HELB . As stated in the empirical review we identified the main factors that influence information security levels in public financing institutions as organizational factors, human factors, socio-cultural factors, technological factors and external environmental factors. Through regression analysis the research discovered that organizational factors, human factors, socio-cultural factors, technological factors significantly influencing level information security. The study further showed public financing institutions in Kenya have not establish comprehensive information security programs by establishing measures to improve information security management in the whole institution, as proposed by ISF (2005b) that linked comprehensive implementation of information security to achieving institutional, strategic and tactical benefits. In summary institution with an evolved Information Security practice that looks into organizational, external environment, socio-cultural, human factors and integrated in enterprise risk management processes provides increased value to their stakeholders.

5.3 Recommendations

The study makes the following recommendations based on the objectives of the study; HELB and other public financing institutions should start to regularly evaluating the levels of information security in their respective institutions. Information security in an organization needs to be quantified to determine what level of security is implemented in the organization and what areas still require attention, and to track the progress of the implementation of security measures as institutions cannot improve on what those do not know.

HELB should look beyond technological methods in solving its information security concerns by including other factors like organizational factors, human factors, socio-cultural factors, and external environment factors.

5.4 Limitation of the research

While conducting the research some observed limitations that could outline some bias to the findings of the research included data collection involved only the staff on the case study organization at the same time some of the questions asked were technical this would mean non-technical staff were not certain with some of their answers. Subject matter is considered sensitive and therefore the respondents may have been conservative with their answers as they consider disclosure to expose there weakness of the institution and also the fact the researcher works in the same institution may be a source of bias towards the study.

5.5 Suggested Areas for Further Research

The study suggests that a study should be replicated in the private sector institutions that deal with public financing like giving loans to the members of the public, such as Savings and Credit Co-operatives (SACCO) also important to conduct a study in such institutions as National Social Security Fund (NSSF), National Hospital Insurance Fund (NHIF) dealing with public savings. Further studies should also be undertaken in Kenyan public institution but to specific factors for example socio-cultural factors in public financing institutions as this study was more of holistic as well as study should be done with the technical staff as the only respondents.

REFERENCES

Breakwell, G. M. (1995) Coping with Aggressive Behaviour Leicester: British Psychological Service.

Canavan, S. (2003). An Information Security Policy Development Guide for Large Companies. SANS Institute.

Chandran, E. (2004). Research Methods: A Quantitative Approach with Illustrations from Christian Ministries.Nairobi: Daystar University.

Cheboi, B. C. (2002). Financing Higher Education: The experience of the Higher Education Loans Board. Paper presented at the First Exhibition by Kenyan Universities held at Kenyatta International Conference Centre, May 2002, Nairobi.

Cooper, D. R. and Schindler, P.S (2011).*"Business Research Methods",* 11th, edition. McGraw-Hill Publishing, Co. Ltd. New Delhi-India

Cronbach, L. J. (1951). Coefficient alpha and the internal structure of tests. Psychometrika 16:297–334.

Dinnie, G. (1999). The Second Annual Global Information Security Survey. Information Management & computer security, Vol. 7, No. 3, pp. 112-120.

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.

Heeks. R (2003). Most e government project for development fail. How can risks be reduced. I government working series. Paper no 4.

Hone, K. & Eloff, J.H.P. (2002). What makes an Effective Information Security Policy. Network Security, Vol. 20, No. 6, pp. 14-16.

Hussain S. J. and Siddiqui M. S, (2005). Quantified Model of COBIT for Corporate IT Governance, Proceeding of First International Conference on Information and Communication Technologies, ICICT, pp. 158 – 163.

Igbaria, M., Zinatelli, N., Cragg, P.B., and Cavaye, A.L. (1997). Personal Computing Acceptance Factors in Small Firms: A St ructural Equation Model, MIS Quarterly, 21, 3, 279-305.

ISO/IEC 27001: (2005), Information technology- Security techniques - Information security management systems- requirements,.

Jarvenpaa, S.L. and Ives, B. (1991). Executive Involvement and participation in Management Information Technology. MIS Quarterly, 15(2), 205-227

Thomson K. L, and. Von Solms R, Information security obedience: a definition, J Computers & Security, Vol. 24, **(2005)**, pp. 69-75.

Kenya ICT Board (2010). Making Kenya a top ten ICT hub. http://www.doitinkenya.com /pdf/BPO%20&%20IT%20SuppFinal.pdf

Kothari C.R. (1990). *Quantitative Techniques.*

Makatiani W. (2012). *We must improve cybersecurity*. http:// www. businessdailyafrica.com/

McKay, J. 2003. Pitching the Policy: implementing IT Security Policy through Awareness. SANS Institute.

Mugenda, A. G. and Mugenda, O M. (2003). Research methods. Quantitative and qualitative approaches. Nairobi: Acts press.

Mungai, M. (1989). University Education in Kenya: Trends and Implications for Cost, Finance and Occupations. Nairobi: Ministry of Education/World Bank.

Mwale (2011). *CCK forms team to fight increased cases of cyber crime.* Retrieved on 15th September 2012 from http://www.ktnkenya.com/business/InsidePage.php?.

Mwiria, K., and Ng’ethe, N. (2002, September). Public university reform in Kenya: Mapping the key changes of the last decade. Unpublished research report. Nairobi.

Nalika, P. (2011).*Kenyan government shifts focus from connectivity to cyber security*. http://www.cio.co.ke/news/main-stories/Kenyan-government-shifts-focus-from-connectivity-to-cyber-security

Ngundi, V (2010). *Cybercrime, cyber security and Privacy***.** (Kenya IG F, 29th July 2010)

Nyabiage(2011). *CCK forms team to fight increased cases of cybercrime*. Retrieved on 15st September 2012 from http://www.ktnkenya.com/business/InsidePage.php?.

Otieno, W. B. (1997). *Programme Performance Evaluation: University Students loans Scheme*. Unpublished M.Ed. thesis, Kenyatta University.

PriceWaterHouseCoopers (PwC) (2011*). Cyber Security M&A: Decoding deals in the global Cyber Security industry*. http:// www.pwc.com /gx/en /aerospace-defence /publications /cyber-security-mergers-and-acquisitions.jhtml

Rodrigo, W., Kirstie, H., Konstantin B. (2009) Human, Organizational and Technological Challenges of Implementing IT Security in Organizations

Schneier, B. (2004). Secrets & lies: Digital security in a networked world. Indianapolis, IN: Wiley Publishing.

Straub, D. W. (1994). The effect of culture on IT diffusion: e-mail and fax in Japan and the US. *Information Systems Research, 5* (1), 23-47.

Straub, D.W. and Welke, R.J. (1998). Coping with systems risk: Security planning models for management decision making. MIS Quarterly, 20 (4), 441-469.

Tarimo, C. N (2006), A Social- Technical View of ICT Security Issues, Trends, and Challenges: Towards a Culture of ICT Security- The Case of Tanzania, *Stockholm University, Department of Computer and Systems Sciences*, December 2006.

Von Solms, R. (1999). Information security management: why standards are important. 7, 1(50-57).

Von Solms R. (2004). A framework for the governance of information security. Computers and Security 2004; 23(8):638–46.

APPENDIX

SECTION A: GENERAL INFORMATION (Please tick as appropriate)

Please do not give your names

1) Please specify your gender Male [ ]

Female [ ]

2) Please specify years you have worked at HELB

a. Below 1 year [ ]

b. 1 to 5yrs [ ]

c. 5 -10 years [ ]

d. 10 years and above [ ]

3) What is your highest level of education?

a. Diploma [ ]

b. Degree [ ]

c. Masters [ ]

d. PhD [ ]

4) Position

a) IT Department Staff [ ]

b) Non IT Department Staff [ ]

5) How do you rate your computer knowledge

a) Excellent [ ]

b) Very Good [ ]

c) Good [ ]

d) Average [ ]

e) Below Average [ ]

2) I understand the general meaning of information security

a) Yes [ ]

b) No [ ]

SECTION B: Please indicate how strongly you agree or disagree with the following statements by marking (X) the appropriate box

	Strongly Disagree	Disagree	Unsure	Agree	Strongly agree
	1	2	3	4	5
Management Support					
1) I am aware the management gives its support to information security process in HELB					
2) The management of HELB prioritizes information security					
Budgeting allocation					
3) I am aware that Information security is part of the overall annual budget for HELB					
4) I am aware that Information security is part of the ICT department budget					
Information security policy enforcement and adaptation					
5) I am aware HELB has a written Information security policy					
6) I have access to the HELB Information security policy					
Awareness					

	Strongly Disagree	Disagree	Unsure	Agree	Strongly agree
	1	2	3	4	5
7) There is appropriate awareness program to ensure that HELB staff are aware of their security responsibility					
8) I am aware that information security awareness exercise are frequently undertaken by HELB					
Organization mission and leadership					
9) HELB has allocated enough qualified staff for enhancing Information security					
10) HELB has a security committee that reports it findings to the management					
Information security training and education					
11) HELB gives regular and structured training program to all members of staff on information security					
12) HELB gives me specific training about information security					

	Strongly Disagree	Disagree	Unsure	Agree	Strongly agree
	1	2	3	4	5
procedures i.e safekeeping of confidential documents that I must follow					
Legislation and law					
13) I am aware of the legal implications of information I have access to					
14) HELB is certified by any international security standards like COBIT, ITIL etc.					
15) I am aware HELB employs international accepted standards like COBIT, COSO,ITL to manage information security					
Socio-ethical awareness					
16) I am aware that the work I do is part of HELB property					
17) I am aware the management considers my personal information as private					
Risk Analysis					

	Strongly Disagree	Disagree	Unsure	Agree	Strongly agree
	1	2	3	4	5
18) I am aware that HELB frequently evaluates the risks to its information systems					
19) I am aware HELB has a specific team of individuals that are responsible for information security.					
20) Risks are communicated to the people who are responsible for resolving the risks.					
Information security Culture (behavior, beliefs,)					
21) I consider Information security as a technical issue and therefore should be handle by ICT staff					
22) I do open all the emails addressed to me even if I do not know the source					
23) Due to my nature of work at times I share my password but do change it					
24) I have limited ability to download applications and install in my					

	Strongly Disagree	Disagree	Unsure	Agree	Strongly agree
	1	2	3	4	5
office desktop machine					
Technological factors					
25) I am aware HELB uses anti-virus to protect its IT systems					
26) I am aware HELB has a firewall					
27) I am frequently made to change my password automatically					
Access control to HELB data					
28) I believe that HELB information and system resources cannot be leaked out to unauthorized person easily					
29) I am aware that HELB information and system resources cannot be altered by unauthorized persons					
30) I am able to account for all the HELB information I have shared with other organizations and customers					
THANK FOR YOUR SUPPORT					