THREATS MITIGATION MEASURES AND SECURITY OF CLOUD BASED ENTERPRISE RESOURCE PLANNING SYSTEMS IN KENYA

KINYANJUI JOHN MUIRURI

A Management Research Project Submitted in Partial Fulfillment of the Requirements for the Award of Master of Business Administration Degree, School of Business, University of Nairobi

OCTOBER, 2015

DECLARATION

This research project is my original work and has not been presented for a degree in any other university.

Signature………………………………… Date…………………………………….

Kinyanjui John Muiruri

D61/64828/2013

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

Signature ………………………………… Date…………………………………….

Mr. Joel Lelei

Department of Management Science

School of Business

University of Nairobi

DEDICATION

This project is dedicated to my parents who encouraged me to begin the Master’s program and supported me both morally and financially throughout my period of study to attain a Master’s degree in Business Administration.

ACKNOWLEDGEMENTS

First and foremost, I thank the Almighty God, for granting me the strength, health and courage to complete this arduous task.

I extend my gratitude and appreciation to my Project supervisor Mr. Joel Lelei for walking with me through the preparation of this paper as well as the University of Nairobi School Of Business for facilitating my coursework and the writing of this paper.

To my classmates without whose interest and co-operation I could not have produced this study. I wish to thank them for supporting this initiative and affording me their time and sharing their experiences.

Finally I appreciate my friends and Family for the support they have given me throughout the writing of this project, whether morally or financially, or through advice and recommendations.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

CCs	Cloud Consumers
CPs	Cloud Providers
CSP	Cloud Service Provider
ERP	Enterprise Resource Planning
ICT	Information and Communication Technology
IDC	International Data Corporate
IIS	Integrated Information System
IT	Information Technology
NIST	National Institute of Standards and Technology
OECD	Organization for Economic Co-operation and Development
SEM	Strategic Enterprise Management
SLA	Service Level Agreement
SMP	Security Management Process

ABSTRACT

Implementation of cloud computing and Enterprise Resource Planning (ERP) Systems has found widespread usage in large and mid-sized institutions worldwide. There has been a rapid increase in implementation of these systems in management and administration of various organizations. Despite the implementation most of the organization have faced various challeges and threats which have become a security issue. This study sought to assess the threats mitigation measures and security of cloud based enterprise resource planning system in Kenya. The specific objectives of the study were to establish the security threat mitigating measures employed by the organizations using cloud based ERP systems and to determine the relationship between security threat mitigation measures and security levels of cloud systems used in organizations. The study adopted a descriptive research design. The design was used in this study because it can answer questions such as "what is" or "what was". The target population for this study included organizations in Kenya that utilize cloud based ERP systems which made a sample size of 53 organizations drawn from across the various sectors of the economy. The study collected primary data using questionnaires. Data was analyzed by the use of descriptive statistics using SPSS and presented through percentages, means, standard deviations and frequencies. Further the data was regressed to obtain t - values , p-values , specific coefficients and intercepts, standard errors among other values at given significance levels. The study found that found that use of two factor authentication for access to data center was the highly used measure in information security. The study also found that use of two factor authentication for access to data center was the highly contributed to the security level. The study concluded that controlled access to data storage centers contributes the most to the security of cloud based enterprise resource planning system followed by third party security validation. The study also concluded that data security levels have improved in that data has been protected from manifestation of viruses. The study recommends that more to be done to establish the compatibility between cloud solutions with enterprises' legacy systems and business needs, as well as the impact of trying or using cloud solutions on organizational culture, staff skills, and work practices. It also recommended that cloud computing adoption processes should be well documented and more attention should be directed at this area to explore the challenges faced in each stage of the process.

CHAPTER ONE: INTRODUCTION

1.1. Introduction

Information and communication technology has rapidly evolved in the recent decades bringing about many changes in the way people live and go about their businesses. For organizations, it is no longer just about the existence of information technology system, but the functionality and efficiency of such a system is of critical essence (Fers, 2010). Initially, application of information technology (IT) activities focused on various independent functions and departments of the organization thereby leading to sub-optimization of the various functions. In the 1990s, organizations started purchasing enterprise resource planning (ERP) systems, which integrate several business functions enabling them to share databases and hence being real time (Davenport, 2011).

Recent developments have however focused on web-enabling ERP systems and making them inter-organizational. The benefits of ERP are undoubtedly visible. The economic barriers to the adoption of the system to greater extent has been reduced by the advent of cloud computing. The objective of this project is therefore to carefully evaluate the extent and importance of implementation of cloud ERP systems, the challenges faced as well as underscore the exposure to information security threats of cloud based enterprise resource planning systems.

1.1.1. Mitigation Measures

This refers to a set of activities, decisions and infrastructure put in place by an entity to reinforce and assure security of information on a web-based environment. Information security breaches have been rapidly rising over the past decade at an alarming level. For this reason, more and more IT companies have realized that they need to develop mitigation measures for their businesses (Kituku, 2012). By employing basic security mitigation measures and following some rules and policies you define for your organization. It is therefore necessary for an organization to develop the necessary mitigation measures. Measures such as access authorization, authentication procedures, firewalls, spy detectors, antiviruses, host-based intrusion detection among others have significant impact in enhancing security of cloud ERP systems.

1.1.2. Security

Security is the act of protection against threats and damages. Information security is the process of protecting the confidentiality, integrity and availability of data from accidental or intentional misuse by people inside or outside an organization or facility. According to Sabahi (2011) key elements of information security include limiting information exclusively to authorized entities; preventing unauthorized changes to or the corruption of proprietary data; guaranteeing authorized individuals the appropriate access to critical information and systems; ensuring that data is transmitted to, received by or shared with only the intended party; and providing security for ownership of information (Mohamed & Pillutla, 2014).

1.1.3.Mitigation Measures and Security Levels

Mitigation Measures of information and information systems can include access authorization, authentication procedures, firewalls, spy detectors, antiviruses among others. For these measures to enhance security, it is imperative that managers of information security at all levels understand their responsibilities and are held accountable for managing information security risk that is, the risk associated with the operation and use of information systems that support the missions and business functions of their organizations (Sabahi, 2011). The complex relationships among mitigation measures and security level of the information systems require an integrated, organization-wide view for managing risk. Unless otherwise stated, references to risk in this study refer to information security risk from the operation and use of organizational information systems including the processes, procedures, and structures within organizations that influence or affect the design, development, implementation, and ongoing operation of those systems (Kshetri, 2012). The role of information security in managing risk from the operation and use of information systems is also critical to the success of organizations in achieving their strategic goals and objectives

1.2. Cloud Computing and Enterprise Resource Planning

Cloud computing is a model for enabling ubiquitous, convenient and on-demand network access to a shared pool of configurable computing resources such as networks, servers, storage, applications and services; that can be rapidly provisioned and released with minimal management effort or service provider interaction. Cloud computing is considered as a recent development in information and communication technology that enables organizations to use new IT development with affordable costs and through minimization of various security threats (Sultan, 2011). ERP system is a business process management software that allows an organization to use a system of integrated applications to manage the business and automate many back office functions related to technology, services and human resources. ERP systems typically operate at the transactional level of the organization (Hyvonen, 2003). The main goal of using an ERP system is therefore to provide a central repository for all information that is shared by all the various facets of the organization and also to provide mitigating measures that protect information from threats, thereby improving the flow of data across the organization with no security interruptions.

Jadeja and Modi (2012), classified the relationship between cloud computing and ERP into three: Software as a service (SaaS) providing applications via internet for example www.salesforce.com; Platform as a service (PaaS) supporting software developers through the whole software life cycle of development, test and deployment for example www.windowsazure.comand; Infrastructure as a service (IaaS) providing the necessary infrastructure by which organizations would not need to purchase servers, datasets and network resources. Jadeja and Modi (2012) further observed that SaaS is the most applicable service through which the necessity for software installation as a common task in in-house IT, will be diminished. The combination of cloud computing and ERP system introduced an era of cloud ERP that is known as an emerging technology that deploys ERP services in a cloud environment.

Implications of cloud computing and ERP software is that it brings users economic benefits during a company's operational management. The benefits are related to sizable cost savings and competitive advantage enhancements (Kituku, 2012). The threats of cloud computing and ERP is resistance by leading ERP vendor to sell the software to business organization and that it is fully reliant on the internet to function. If your wireless router should malfunction or internet provider is unable to offer service for some reason, you will lose access to all of your ERP data until the system is restored.

1.3. Information Security

Information security is the practice of defending information from unauthorized access, use, disclosure, disruption, perusal, inspection, recording or destruction. Organizations and people find it highly imperative to secure information and data due to their sensitive nature and value in decision-making (Sabahi, 2011). With the widespread of cloud computing, various IT organizations, experts and users have expressed concerns over critical security issues. These concerns originate from the fact that in a cloud-computing environment, data is stored remotely from the customer's location; in fact it can be stored at any location. Security in particular is one of the most argued about issues in cloud computing environment; several enterprises look at cloud computing warily due to projected security risks.

1.3.1. Security Threats

Security threat can be defined as possible danger whose occurrence might exploit the vulnerabilities of a system and thus cause possible harm. Information systems' security threats may occur in many different ways; for example denial of service attacks, identity theft, theft of information, unauthorized access to information storage areas, information leakage, information alteration among others. Cloud computing is a network-based environment that focuses on sharing computations and resources. Cloud service providers use virtualization technologies combined with self-service abilities for computing resources via network infrastructure (Kshetri, 2012).

Security concerns of users of cloud services may also substantially vary based on the type of cloud platform on which they are. There are essentially three cloud platforms that users may make use of; public, private or hybrid. In a public environment, providers make several computing resources such applications and storage available to the public (Cornford & Pollock 2004). Private cloud refers to internal service of a business that is not available to external parties. Private cloud is essentially a marketing term for architecture that provides hosted services to a particular group of people behind a firewall. In a hybrid platform, a company provides and controls some resources internally and has some others for public use.

Various researchers have identified possible reasons that contribute to the vulnerabilities of cloud platforms. For instance, Mavodza (2012) observed that the real snag for the current cloud-computing environment is that there are no interoperable cloud provider standards yet for security functions to protect those knowledge assets. This is confirmed by David, (2009) who pointed out that this is a currently on-going discussion that cites the issues, challenges and possible solutions in making the standardization achievable. Kshetri, (2012) pointed out that one of the reasons that could possibly raise the issues of security concern from the customers point of view, is the temptation by the global service providers to use cheaper hosting services for developing counties thereby exposing them to attacks by cyber criminals who may take advantage of the loopholes.

1.3.2. Security Threat Mitigation Measures

A threat, in the context of computer security, refers to anything that has the potential to cause serious harm to a computer system. A threat is something that may or may not happen, but has the potential to cause serious damage. Threats can lead to attacks on computer systems, networks and more (Mohamed & Pillutla, 2014). Threats are potentials for vulnerabilities to turn into attacks on computer systems, networks, and more. They can put individuals' computer systems and business computers at risk, so vulnerabilities have to be fixed so that attackers cannot infiltrate the system and cause damage. Threats can include everything from viruses, trojans, back doors to outright attacks from hackers. Often, the term-blended threat is more accurate, as the majority of threats involve multiple exploits. For example, a hacker might use a phishing attack to gain information about a network and break into a network.

Security measures involve a set of activities, decisions and infrastructure put in place by an entity to reinforce and assure security of information on a web-based environment. Information/data security in the context of cloud ERP is of critical essence and hence a key consideration in deciding whether to adopt a private, public or hybrid cloud platform. All organizations and people are driven by the need to have sensitive information about them protected from leakage, unauthorized access/alteration, loss or destruction by the use of measures such as use of two factor authentication for access to data center was the highly used measure in information security (Almorsy, Grundy and Mueller, 2010).

In literature, researchers have found a threat to information security known as an insider threat. According to Steele and Wargo (2007), insiders are as much a threat to the information security of an organization as outsiders, but organizations are not implementing the necessary countermeasures to address these threats. Colwill (2009) quantifies this somewhat, noting that there has been an overreliance on technical solutions to information security problems, without sufficient consideration of the other factors involved. CSO Magazine (2011) states in their Cybersecurity Watch Survey that insider attacks are more damaging than attacks from an external party, even though insider attacks make up only 22% of total security breaches. Verizon Business (2011), on the other hand, posits in their data breach report that 17% of security breaches are insider related. However, they do not offer any position on the level of damage done by insider attacks. Widup (2010) offers a different perspective on the insider incidents, noting that at least half of them were shown to be accidental and thus requires mitigating measures to enhance information security.

1.3.3. Relationship between Threat Mitigation Measures and Levels of Cloud Based Enterprise Resource Planning Systems

The research model of this study is to establish the security threats, measures and levels of cloud based ERP systems as well as establish the relationship between security measures and security levels. Various security factors/elements of computing systems have been identified including data centres, servers, applications and platforms, networks and data/information. Measures that can be taken to enhance security of these aspects of computing vary in nature and scale. It is the informed view of this research that there exists a direct relationship between security measures in place and security levels of a system and that; existence of controls, procedures, regulations and other design parameters will significantly enhance security of data and infrastructure of cloud systems (Mohamed & Pillutla, 2014). Measures such as access authorization, authentication procedures, firewalls, spy detectors, antiviruses, host-based intrusion detection among others have significant impact in enhancing security of cloud ERP systems.

ERP security solutions have been proven to work, with companies using this method reporting significant decreases in malware incidents, website compromises, data loss and data exposure, security related downtime, and audit deficiencies, according to a May 2010 study by the Aberdeen Group. Turning to security in the ERP should be the first line of defense of an integrated security strategy (Kotb and Roberts, 2011). Implementing firewalls, strong passwords, built-in device security offered by manufacturers and staff education (e.g., protection of passwords and of devices themselves) are also essential elements of "defense in depth." Taking such a comprehensive approach helps ensure the security of the enterprise’s network. See the link for more information about security in the cloud.

1.4. Cloud Computing and Enterprise Resource Planning in Kenya

In Kenya the information technology has been on the rise as the country keeps modernizing. This has been facilitated by the adoption of IT by the neighboring countries. The Kenya Communications Act (KCA) of 1998 established the National Communication Secretariat (NCS), headed by a Communication Secretary, whose main objective is to advise the government on the adoption of an IT policy, which, among other things is meant to encourage competition in the provision of technological advances (Klein 2003). Historically, it has not been clear which arm of government deals with matters relating to IT or who is responsible for the regulation of the IT sub-sector. However, the national ICT policy approved in January 2006 recognizes CCK as the regulator of the whole of the ICT sector, including IT and broadcasting. (Kebs, 2012).

Cloud computing relies on real time server interactions with low latency, high bandwidth, and a stable connection that are largely lacking in most of Africa. This problem is compounded with the lack of cheap computing devices and low computing literacy levels where most people on the continent cannot even perform the most basic functions (McLaughlin 2008). Many companies have invested in Cloud Computing ERP system technology by building their public clouds, which include Amazon, Google and Microsoft. These companies are often releasing new features and updates of their services. For instance, Amazon Web Services (AWS) released a Security and Economics centre on their website to have academic and community advice regarding these issues (Khajeh-Hosseini et al., 2010b). This shows that there are still lots of doubts about the costs and security for enterprises to adopt Cloud Computing and ERP systems. Hence, the issues of economics and security in Cloud Computing and ERP for enterprises must be researched and implemented.

There are various challenges the organizations are facing with regard to cloud computing and ERP (Daniel, 2008). The challenges include the security worries Enterprise information are important in an information sharing world and the loss of customers' private information such as credit card details can be detrimental to a company. The security of such data especially when stored by a third party is a major concern to companies considering adopting cloud computing. Privacy is another matter (Robinson, 2009). When someone uses these cloud computing services, data is stored on someone else's server and not one's own hardware, and therefore, the user loses some control over the data. In addition to the above, Africa is faced by a unique set of challenges. Internet connectivity is still not available in large parts of the continent.

Many organizations in Kenya struggle with their current systems' architecture that produce inaccurate data and require redundant or manual processes. As a result, IT staffs often spend significant time maintaining obsolete or disparate systems instead of creating new value or implementing strategic applications (Marston, 2011). Crimson Technologies offers ERP solutions that are open, capable and affordable, and that can help organizations realize value from their investment quickly.

1.5. Research Problem

Cloud Computing and ERP are technological platform that allows users, organizations or individuals, to access and use computer resources via the internet on demand independent of device and location (Schubert, 2011; Marston, 2011). Cloud computing has a number of distinguishing characteristics. The provider holds the computing resources. Computing resources are accessible over the Internet via personal computers, laptops, smart phones, and personal digital assistants. With a commercial cloud-computing provider, resources are normally available, for a set fee, based on usage. For the majority of cloud vendors that charge for cycles or time used, an accounting and billing procedure is needed, with contractual terms agreed upon before service is granted (David, 2009).

Globally, a couple of researchers have worked in the area of security in the ERP systems. However, research is still ongoing as more and more vulnerabilities, threats, risks and security challenges emerge with time. In a research conducted by Marston, (2011) cloud computing and Enterprise resource planning (ERP) system security must be governed by the same principles as conventional information security. An ERP system controls all the business related information of an organization as well as information relating to customers and suppliers. It is necessary to protect this information from the opposition as well as to ensure that the information within the ERP system conforms to auditing standards. According to Dhillon, information security has traditionally been an afterthought, even within ERP systems. Because of businesses' increased dependence on information, security is increasingly being considered proactively. While designing, developing and implementing systems, there are enthusiastic discussions of the relevance of certain controls and the hindrance of such controls to the conduct of business and the efficiency of certain security tools

In Kenya, the adoption of technologies has been studied with most focusing on the adoption of ICT in banks such as ICT banking in Kenyan commercial banks. Kahigu (2010), for instance, did a study on the enabling role of ICT in the business re-engineering, a case of KCB. His recommendation was that commercial banks should not be hesitant to implement radical changes as ICT can actually lead to improved cost management and customer care and thus leading to production efficiency. Organizations should seek to change entire organization as opposed to some departments. Musyoka (2009) did a survey of the factors influencing choice of ICT systems for core banking activities in Kenya. He found that cost, size of the organization were among the factors affecting adoption of ICT. He recommended that organizations should have adequate capital in the case where they independent any kind of technology. Kitur (2011) did a survey of the strategic role of ICT systems among insurance companies in Kenya. He established that IT played a bigger role offering services to the customers and in the operation efficiency of the firm.

A survey of application of ICT for competitive advantage of firms listed at the NSE was done by Vishal (2009) and Lelei (2008) did a study of ICT as a strategic tool in microfinance institutions in Kenya. The findings of these studies indicated that many of the studied companies and organization had implemented ICT in their operations but they were yet to install the ERP systems. None of these local studies looked at the threats mitigation measures and security of cloud based enterprise resource planning system in Kenya. This research, therefore intend to fill this gap regarding the security of Cloud based ERP by addressing the following research question: what are the security threat mitigating measures employed by the organizations using cloud based ERP systems and what is the relationship between security threat mitigation measures and security levels of cloud systems used in organizations?

1.6. Research Objectives

The general objective of this research project is to assess the threats mitigation measures and security of cloud based enterprise resource planning system in Kenya

The specific objectives of the study are to:

(i) Establish the security threat mitigating measures employed by the organizations using cloud based ERP systems in Kenya

(ii) Determine the relationship between security threat mitigation measures and security levels of cloud systems used in organizations in Kenya

1.7. Value of the Study

The findings of the study will help enrich understanding of the relationship between information security threats and mitigating measures of ERP. In addition it is beneficial to practice. Several parties will be interested with the study: Firstly, the study will valuable to the government as it might find it useful in getting an insight on how to foster the development and sustenance of ERP system and cloud computing in Kenya.

Secondly, scholars will find the study useful, as it will act as a foundation for further research as they seek to improve and develop a better understanding of technology acceptance theories and attitudes towards cloud computing acceptance. Lastly, the findings of the study will influence an organization to adopt cloud computing. The reasons for adopting cloud computing and ERP should aid in strategic planning, by both cloud providers and by organizations that could consider using cloud computing assets to meet current or future computing and data and information management needs.

CHAPTER TWO: LITERATURE REVIEW

2.1. Introduction

Cloud computing is an exciting technological breakthrough and a compelling discipline that has already exhibited profound implications on how we work, collaborate and share knowledge, (Mohamed & Pillutla, 2014). The platform represents a fundamental shift in the delivery of information and technology (IT) services that has permanently changed the computing landscape. This chapter presents a review of various research findings and expert opinions and observations about the context of cloud ERP deployment.

2.2. Theoretical Background

This research was based on Diffusion of Innovations Theory, Information Systems Success Model Theory, TAM Model Theory, and Theory of Planned Behavior. These theories were discussed below.

2.2.1. Diffusion of Innovations Theory

Diffusion of Innovations (DOI) Theory was coined by Rogers in 1962 and later revised in 2003. It is a widely used theory in social science disciplines. The theory has its basis in communications and seeks to explain how an idea or product gains momentum and spreads through a specific population or social system. The theory is useful to both the developers and users of ERP systems in evaluating the various mitigating measures that can be applied to counter these threats imposed by the new innovations in the organization. With innovation and deployment of ERP systems in management of organizations in Kenya interpreted as an innovative strategy in the study, various organizations are assumed to have undergone the first, second, and third processes in the diffusion of innovations theory as advanced by Rogers (2003).

These include gathering knowledge about the ERP systems, mitigating measures, persuading stakeholders to support the selected systems in automating their organizational operations and making the decision to implement the systems. While guided by the diffusion of innovations theory, the researcher will seek to establish the organizational experiences during the implementation phase of the ERP systems in public organizations in Kenya. This will help them to finding lasting measures on information security.

2.2.2. Information Systems Success Model Theory

The research study employed use of the Information Systems Success model theory. The information systems success model theory as advanced by Delone & McLean (2003) is based on earlier research in communications by Shannon and Weaver as well Mason's theory on Information Influence. The theoretical model makes use of a causal relationship to analyses success of implementation of information systems in organizations. The information model will be useful in studying cloud computing and ERP systems management their usage in public organizations in Kenya. By using the model, the objectives of the research study will be best addressed to ascertain not only information security threats but also mitigation measures of these threats in management of public firms and organizations.

2.2.3. TAM Model Theory

Davis (1986) proposed the original version of TAM based on the Theory of Reasoned Action (Fishbein and Ajzen, 1975) for testing how users come to accept and use information systems. TAM has become one of the most widely used models in the information system field, partly because of its understandability and simplicity (King and He, 2006). Referring to Lee, Li, Yen, and Huang (2010), TAM enables an organization to grasp the effects of external variables concerning the causal relationship between Perceived Usefulness (PU), Perceived Ease of Use (PEOU), and Behavioral Intention (BI); it thereby helps the organization with implementation and application of technology systems. This theory is important to the current study in that it help the motive behind organization adoption of cloud computing and ERP systems. The theory helps in assessing the threats that occurs as a result of adopting the ERP systems.

2.2.4. Theory of Planned Behavior

The Theory of Planned Behavior (TPB), the theory states that attitude toward behavior, subjective norms, and perceived control, together shape an individual's behavioral intentions and behaviors, TPB extends the theory of reasoned action (TRA) by adding perceived behavioral controls to the model, including attitude, subjective norms, behavioral intention, and actual behavior (Madden, Ellen, & Ajzen, 1992; Yi et al., 2005). TRA is a model for the prediction of behavioral intention, spanning predictions of attitude and predictions of behavior. TPB and TRA are relevant to this study because they will assist in prediction of individual behavioral intentions to the acceptance and usage of cloud computing and ERP system in the Kenya.

2.3. Enterprise Resource Planning Systems

An enterprise resource planning system is an enterprise wide-information system that integrates and controls all the business processes in the entire organization (Al-Fawaz, Zahran, and Tillal, 2008). The systems are considered as an integral information solution or practice connected information system or integrated application package which help in controlling organization functions through unified information structure (Fers, 2010). As an organization's operations become spread in size and space, the requirement for coordination becomes increasingly of significant importance. Size and complexity makes concerns about new management technology pertinent and often, information technology such as integrated enterprise resource planning systems is considered a solution to this trend.

Security problems exist in every facet of an ERP system. These facets can be classified into three categories: network layer, presentation layer, and application layer, which include business processes, internal interfaces, and database. When a customer/partner communicates with an ERP system, or the business components located in different places interact with each other, the security problems in these cases are classified into the network security domain. ERP experts will not deal with these cases directly, instead this function will be provided by purchasing from other vendors who are experts at network security (Foster et al., 2008). The presentation layer refers to the graphical user interface, browsers, and PCs. Since the transmission of GUI packets is impossible to restrict, ERP experts cannot secure the system by limiting user access to GUI. The better way to provide security may be to place a CITRIX server between the user and the ERP system. The security in application layer invests large efforts of the ERP experts to offer an effective way to secure the business data and processes. The technicians will also choose to activate/deactivate the security functions provided by the database vendor according to the overall security solution.

2.4. Cloud Computing

Cloud Computing is a term used to describe both a platform and type of application. As a platform, it supplies, configures and reconfigures servers, while the servers can be physical machines or virtual machines. On the other hand, Cloud Computing describes applications that are extended to be accessible through the internet and for this purpose large data centers and powerful servers are used to host the web applications and web services (Boss et al., 2007). The cloud is a metaphor for the Internet and is an abstraction for the complex infrastructure it conceals. There are some important points in the definition to be discussed regarding Cloud Computing. Cloud Computing differs from traditional computing paradigms as it is scalable, can be encapsulated as an abstract entity which provides different level of services to the clients, driven by economies of scale and the services are dynamically configurable (Foster et al., 2008).

There are many benefits stated of Cloud Computed by different researchers which make it more preferable to be adopted by enterprises. Cloud Computing infrastructure allows enterprises to achieve more efficient use of their IT hardware and software investments. This is achieved by breaking down the physical barrier inherent in isolated systems, automating the management of the group of the systems as a single entity. Cloud Computing can also be described as ultimately virtualized system and a natural evolution for data centers which offer automated systems management (Basoglu, Daim, Kerimoglu, 2007). Enterprises need to consider the benefits, drawbacks and the effects of Cloud Computing on their organizations and usage practices, to make decision about the adoption and use.

2.5. Cloud Enterprise Resource Planning

Cloud ERP is an approach to enterprise resource planning (ERP) that makes use of cloud computing platforms and services to provide a business with more flexible business process transformation. For many businesses the biggest investments they make are in human resources, inventory and fixed assets and managing those resources are what ERP is all about (Foster et al., 2008). Empowering your people, taking control of your business and playing to your strengths are the core areas where the Acumatica Cloud ERP suite of business applications can help your organization grow profitably by allowing your people to work anywhere, anytime on any device via our web browser based accounting, inventory management and financial management applications.

Some of the key enterprise functions that ERP systems support include supply chain management, inventory management, sales and customer relationships management, financial and cost management, human resource management among others (Sofa, Golany & Dori, 2002; Sedeta *et al*, 2004). The integration of these functions is critical to the success of an organization. Over time, enterprises have attempted to achieve this coordination by increasingly investing in state of the art information and communication technologies (ICT). The high cost of deploying a robust ICT framework such as ERP systems and maintaining them in-house has for a long time held back other organizations from adopting the system despite understanding their benefits (Boss et al., 2007). The breakthrough came with the development of cloud environment that enables organizations to enjoy the services on a pay-as-you-use basis, as well as transferring the storage and maintenance operations to third parties. The deployment of ERP systems on a clod platform has considerably brought down the computing costs and ensured that more organizations can enjoy the benefits of such systems within the limits of their budgets.

2.6. Threat Measures and Levels in Cloud Enterprise Resource Planning Systems

Security threat can be defined as possible danger whose occurrence might exploit the vulnerabilities of a system and thus cause possible harm. Threats can occur/take various forms. Their impact may also range from minor to major depending on how the risk at hand is viewed; and the sensitivity, confidentiality and value attached to the information that may be lost, leaked or damaged in the event of their occurrence (Kim, 2009). Security measures include a defined set of strategies, procedures, controls and design aspects put in place by stakeholders in order to guard against occurrence of threats or at least reduce their impact in case of their occurrence.

Security of information/data is a matter of crucial importance to the users of computing technologies. Security is considered as one of the top ranked open issues in adopting cloud computing model, as reported by International Data Corporate (IDC, 2010). A reasonable justification of such increasing concerns of the cloud consumers (CCs) about cloud security includes: (1) The loss of control over cloud hosted assets (cloud consumers become not able to maintain their Security Management Process (SMP) on the cloud hosted IT assets); (2) The lack of security guarantees in the service level agreements between the cloud providers(CPs) and cloud consumers; and (3) the sharing of resources with competitors or malicious users, (Almorsy, Grundy & Mueller, 2010).

IT security in general has experienced intense changes over the past decade. Computerized tasks and processes have created increasing vulnerabilities in the workplace, networked devices have introduced new threat paths, and the ever-growing volume of personal and financial information stored in binary form has triggered waves of privacy concerns from organizations as well as individuals. The electronic giant Sony and the world’s largest tech-security company RSA Security experienced massive security breaches (Medlin, 2001). Seeing these systems in a private, closed environment being victims of online attacks, it is natural for one to wonder why cloud services would be any more secure.

To mitigate these concerns, cloud service providers are taking a great effort to build secure platforms that meet today’s strict security standards. These standards, however, have very little effect on the protection customers receive: The standards are merely a measurement of level of assurance that the certifications entail (Boss et al., 2007). For example, applications hosted in a HIPAA-compliant cloud platform still could face security breaches if the application’s architecture and deployment are not handled with a full understanding of the limitations and constraints of the cloud platform. Similarly, a FISMA-certified cloud platform simply means the cloud service provider is compliant with applicable federal law for storing data for government agencies, and does not guarantee the data is perfectly safeguarded (Medlin, 2001).

2.7. Empirical Review

ERP systems have found widespread usage in large organizations across various continents. To keep up with the management demands in the 21st century as observed by Nyandiere et al (2012), organizations have turned to ERPs to replace their legacy systems and to address the security threats involved. Though initial implementation was observed in manufacturing industries, organizations have taken up the systems to provide institutional-wide automation for their processes (Ferrell, 2003). This has aided them automate their core business areas in business administration, finance, staffing, client management among others. On implementation, these systems are anticipated to provide increased efficiency and effectiveness of processes, reduce overhead costs in ICT, improve decision making, improve resource management as well as building business innovation while supporting strategic change (Sullivan and Bozeman, 2010). With all these benefits organizations have been able to counter the threats posed by these ICT improvements i.e. cloud computing and ERP systems.

As argued by Davenport (2003), ERP systems provide seamless integration of all information flowing through a company's departments. With the seamless integration of information within institutions, managers are able to overcome threats that are emanating from incompatible systems and inconsistent operating practices. Acquisition of these systems may be through commercial off-the-shelf systems or custom designed systems in line with an organizational needs. Past studies in implementation of ERP systems in business organizations have focused more on the benefits that an organization can derive from adopting an ERP system. However, more literature on threats and challenges facing these implementation experiences needs to be highlighted to inform current and future adoption of ERP systems in organizational administration (Yetton and Sharma, 2003).

According to Verville and Halingten (2003), ERP systems are used to connect back-office operations such as manufacturing, financial and human resources into one system. In the current decade, enterprise resource planning has evolved to a suite of application modules that are used to link back-office operations to front-office operation as well as internal and external supply chains. They conjoin functional areas and business processes in a seamless integrated environment. This provides a wider scope for applicability to organizations. Enterprise Resource Planning systems have gained widespread usage in large corporations and institutions across the globe.

Pollock (2004) in a study aimed on ERP systems use in a UK organizations points out that the uniqueness of an organization set up makes most business ERP systems incompatible with their functions. This necessitates a custom development of a system compatible with the structure and functions of a specific organization. The choice of either a custom development or adoption of a readily available system should be informed by a thorough systems analysis and design evaluation while putting the organizational strategic objectives into consideration (Basoglu and Kerimoglu, 2007). This can be achieved by drawing up an elaborate implementation framework to guide the process and establish mitigating measures to counter the incompatibility of the ERP system.

2.8. Summary

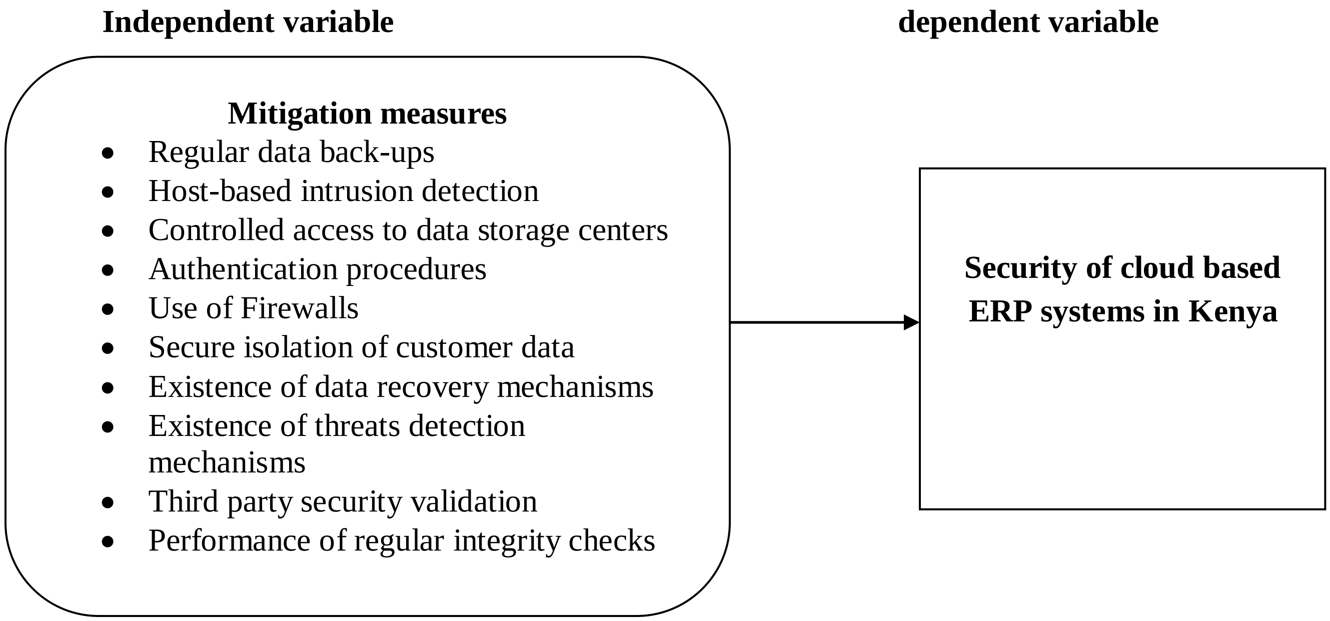
In the last decade as argued by Pollock (2004), there has been a rapid increase in implementation of ERP systems in management and administration of many organizations and firms. In this regard, organizations have turned to ERP systems to replace existing management and administration computer systems. In analyzing rollout of ERP systems in Public organizations, focus has been placed on security threats, security levels and mitigating measures that have been applied in Security of cloud based ERP systems in organizations.

To achieve the objectives, the study has utilized the several theories to provide a detailed examination of security threats and mitigating measures of ERP systems in Kenyan organizations and firms. The theoretical basis and empirical review brought out in the study also influenced the formulation of the illustrated conceptual framework which will guide the entire research study

2.9. Conceptual Framework

In this research, the conceptual framework is the concise description of the phenomenon under study accompanied by visual depiction of the variables under study (Mugenda, 2008). The independent variables include the mitigation measures which include Authentication procedures, Use of Firewalls, Controlled access to data storage centers, Regular data back-ups, and host-based intrusion detection while the dependent variable is security of cloud based ERP systems in organizations. The conceptual framework of this study is represented by Figure 2.1.

Figure 2.1. Conceptual framework



Independent variable

dependent variable

Mitigation measures

- Regular data back-ups
- Host-based intrusion detection
- Controlled access to data storage centers
- Authentication procedures
- Use of Firewalls
- Secure isolation of customer data
- Existence of data recovery mechanisms
- Existence of threats detection mechanisms
- Third party security validation
- Performance of regular integrity checks

Security of cloud based ERP systems in Kenya

Source: Author 2015

CHAPTER THREE:RESEARCH METHODOLOGY

3.1. Introduction

This chapter sets out the research methodology that the researcher sought to adopt so as to meet the objectives of this study. The chapter describes the research design, the population, sample and sampling techniques, data collection and analysis methods to be used as well as models of presentation of the findings.

3.2. Research Design

The research study adopted a descriptive research design. Descriptive research design was used in this study because it can answer questions such as “what is” or “what was”. A descriptive research is also used in a study to examine a phenomenon that is occurring at a specific place(s) and time and elicit recommendations. The choice for use of descriptive research design was to provide a comparative approach to the use of enterprise resource planning systems in integrating management of organizations in Kenya against a backdrop of other success cases in developing and developed nations. This also helped the researcher in using comparative statistical methods to analyse the research subject in the selected group of firms that make use of cloud ERP systems.

3.3. Target Population

The target population for this study included organizations in Kenya that utilize cloud based ERP systems. In a baseline survey on cloud, computing in Kenya carried out by Omwansa, Waema and Omwenga (2015), a total of 265 organizations were identified as possible participants in cloud computing research. This research therefore assumed a population size of 207 organizations.

3.4. Sampling Design

The study used stratified random sampling techniques. A stratified random sampling involves the division of a population into smaller groups known as strata. The strata are formed based on members' shared attributes or characteristics. A random sample is taken from each stratum. The strata in the study came from 265 organizations. Stratified random sampling was used to achieve equal representation of organizations with cloud computing ERP in Kenya. According to Mugenda and Mugenda (2003), a sample size between 10% and 30% of the target population is considerably representative and is viable in social science studies. The study utilized a sample of 53 organizations drawn from across the various sectors of the economy. This represented 20% of the target population. The sampling frame was as presented in Table 3.1 below

Table 3.1: Sampling frame

Category	**Sample**
Government entities	8
Financial institutions e.g. *banks, insurance firms, co-operative societies, building societies, micro-finance*	8
Educational institutions e.g. *universities and colleges*	4
Health-care and allied services e.g. *hospitals and pharmaceutical firms*	4
Agricultural firms- *coffee, tea promotions agencies*	2
Manufacturing entities	8
Communication &Technology firms	3
Professional firms	3
Insurance firms	4
Consulting firms	4
Others service firms e.g. *supermarkets, motor care, hospitality & leisure*	5
Total	**53**

3.5 Data Collection

The study collected primary data using questionnaires. The data collected was qualitative. The questionnaire was designed to collect qualitative data. The questionnaires were administered on a ‘drop and pick later’ technique. Every effort was made to ensure personal delivery and administration of the instrument in order to ensure a higher return rate of the questionnaires. The respondents included the top management in the various organizations which included the managing director, and the information security manager. The questionnaire consisted of four sections. Section A addressed demographic information, Section B addressed the security measures, and Section C established the relationship between security measures and security levels.

3.6. Data Analysis

Objective one: Establish the security threat mitigating measures employed by the organizations using cloud based ERP systems. For this objective the researcher collected data on the various mitigating security measures such as access authorization, authentication procedures, firewalls, spy detectors, antiviruses among others. The data was analyzed by the use of means and standard deviation.

Objective two: Determine the relationship between security threat mitigation measures and security levels of cloud systems used in organizations. For this objective the researcher collected data that established the relationship between measures and security levels of cloud systems used in organizations. The data was analyzed by the use of the following regression model.

The study adopted the following regression model:

$$y = \beta_0 + \beta_1X_1 + \beta_2X_2 + \beta_3X_3 + \beta_4X_4 + \beta_5X_5 + \beta_6X_6 + \beta_7X_7 + \beta_8X_8 + \beta_9X_9 + \beta_{10}X_{10} + e$$

Where: Y = Security of cloud based ERP systems in organizations

β_0 = Constant Term

β_1, β_2, β_3, β_4, $\beta_{5,}$ β_6, β_7, β_8, β_9, β_{10} = Beta coefficients

X_1= Regular data back-ups

X_2= Host-based intrusion detection

X_3= Controlled access to data storage centers

X_4= Authentication procedures

X_5= Use of Firewalls

X_6=Secure isolation of customer data

X_7=Existence of data recovery mechanisms

X_8= Existence of threats detection mechanisms

X_9= Third party security validation

X_{10}= Performance of regular integrity checks

e = error term

CHAPTER IV: DATA ANALYSIS AND INTERPRETATION OF RESULTS

4.1 Introduction

This chapter presents data analysis and discussions. The study had two objectives namely; establish the security threat mitigating measures employed by the organizations using cloud based ERP systems in Kenya and to determine the relationship between security threat mitigation measures and security levels of cloud systems used in organizations in Kenya. The research was conducted on sample size of 53 respondents out of which 40 respondents completed and returned the questionnaires duly filled in making a response rate of 75%. Mugenda and Mugenda (1999) stated that a response rate of 50% and above is a good for statistical reporting. The data was thereafter analyzed based on the objectives of the study. The findings were presented as per the different classes underlined below in percentages.

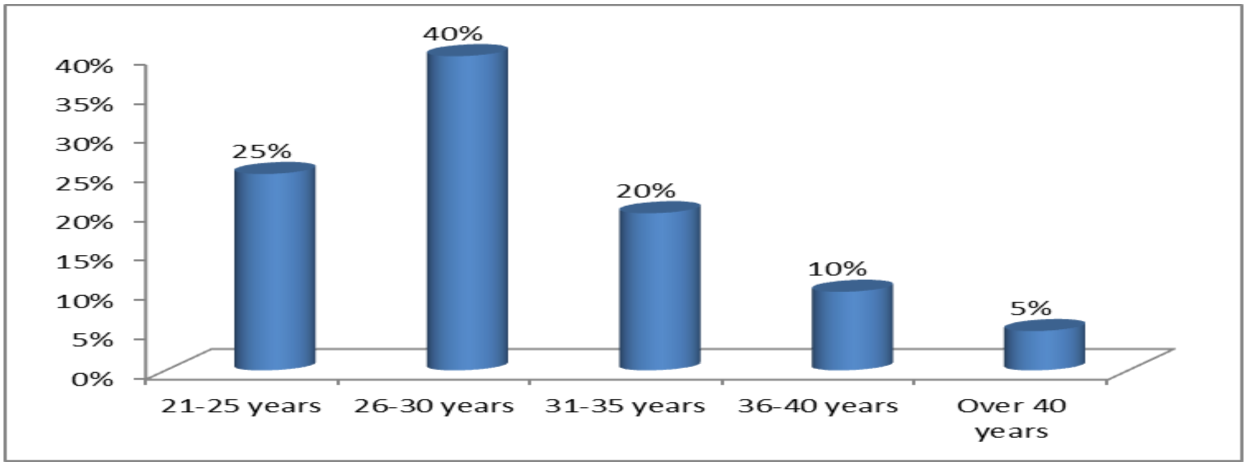
4.2 Demographic Information

The study sought to ascertain the background information of the respondents involved in the study, which included; age of the respondent, gender, position in the organization, duration of work in the organization, number of employees, length of operational of the organization, ownership of the organization and sectors in which the organization fall. The background information points at the respondents' suitability in answering the questions.

4.2.1. Age of the Respondents

The respondents were requested to indicate their age. The findings were as shown in Figure 4.2

Figure 4.2.Age of the Respondents

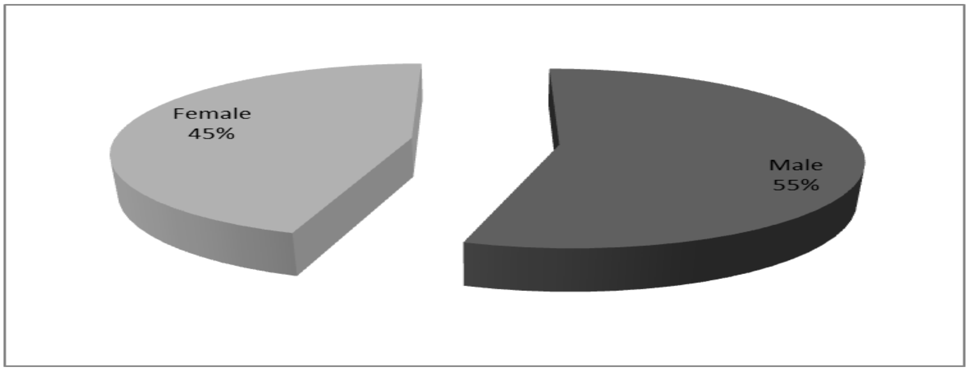


From the findings in Figure 4.2, 40% of the respondents indicated they were between the age of 26-30 years, 25% indicated between 21-25 years, 20% indicated between 31-35 years, 10% indicated 36-40 years while 5% indicated over 40 years. This implies that majority of the respondents were between the age of age of 26-30 years.

4.2.2. Gender of the Respondents

The respondents were asked to indicate their gender. The findings were as shown in Figure 4.3

Figure 4.3. Gender of the Respondents

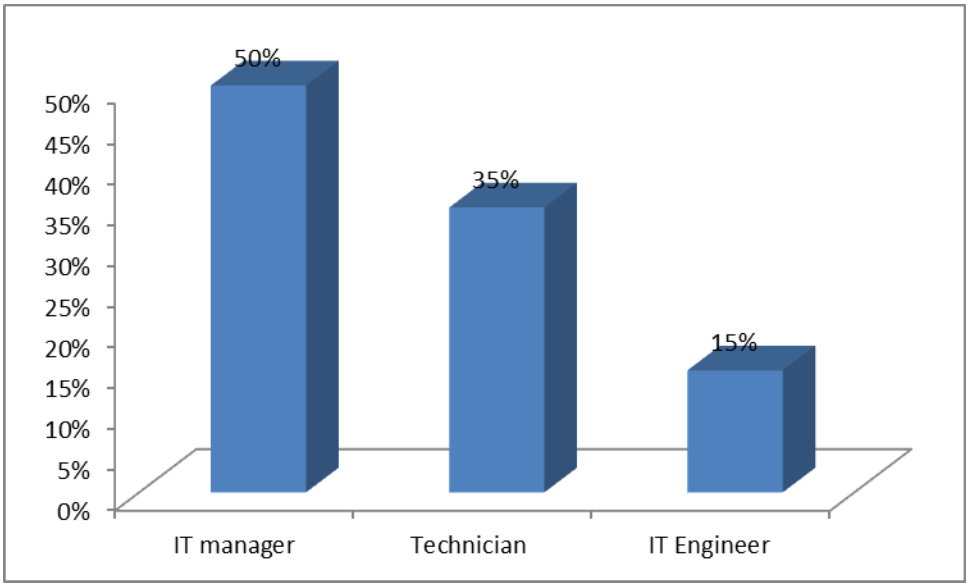


From the findings in Figure 4.3, 55% of the respondents were male while 45% were females. This depicts that majority of the respondents were males.

4.2.3. Position in Organization

The respondents were requested to indicated the position they held in their organization. The findings were as shown in Figure 4.4

Figure 4.4. Position in Organization

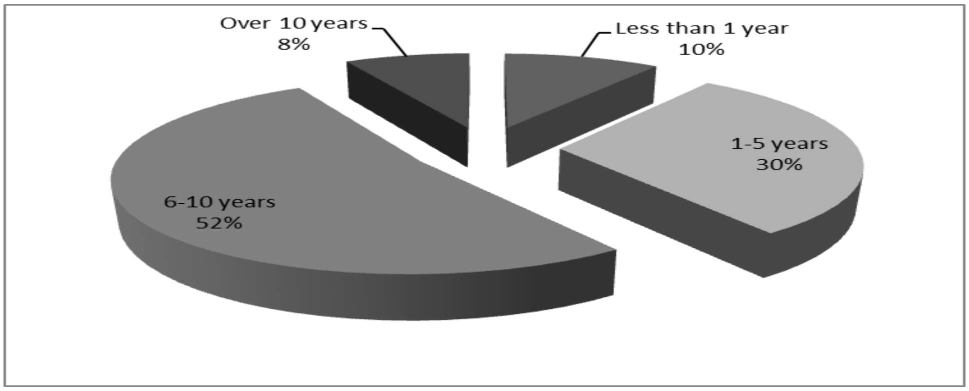


From the findings in Figure 4.4, 50% of the respondents indicated they were IT managers, 35% indicated they were technicians while 15% indicated they were IT engineers. This depicts that majority of the respondents were IT managers.

4.2.4. Duration of Work

The respondents were requested to indicate the lengths of time they have been working in the organization. The findings were as shown in Figure 4.5

Figure 4.5. Duration of Work

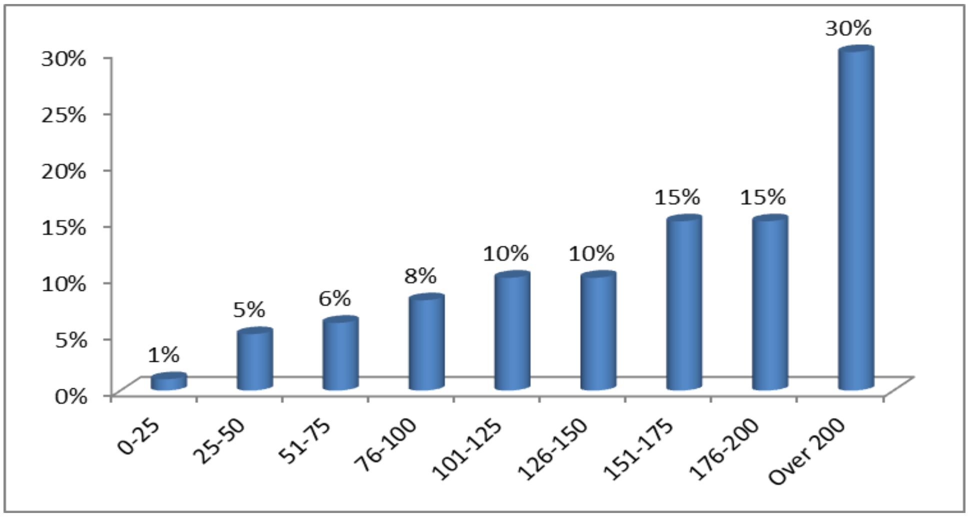


From the findings in Figure 4.5, 52% of the respondents indicated a duration of 6-10 years, 30% indicated 1-5 years. 10% indicated less than a year while 8% indicated over 10 years. This depicts that majority of the respondents had worked in the organization for a period between 6-10 years.

4.2.5. Number of Employees in the Organization

The respondents were requested to indicate the number of employees in their organization. The findings were as shown in Figure 4.6

Figure 4.6. Number of Employees in the Organization

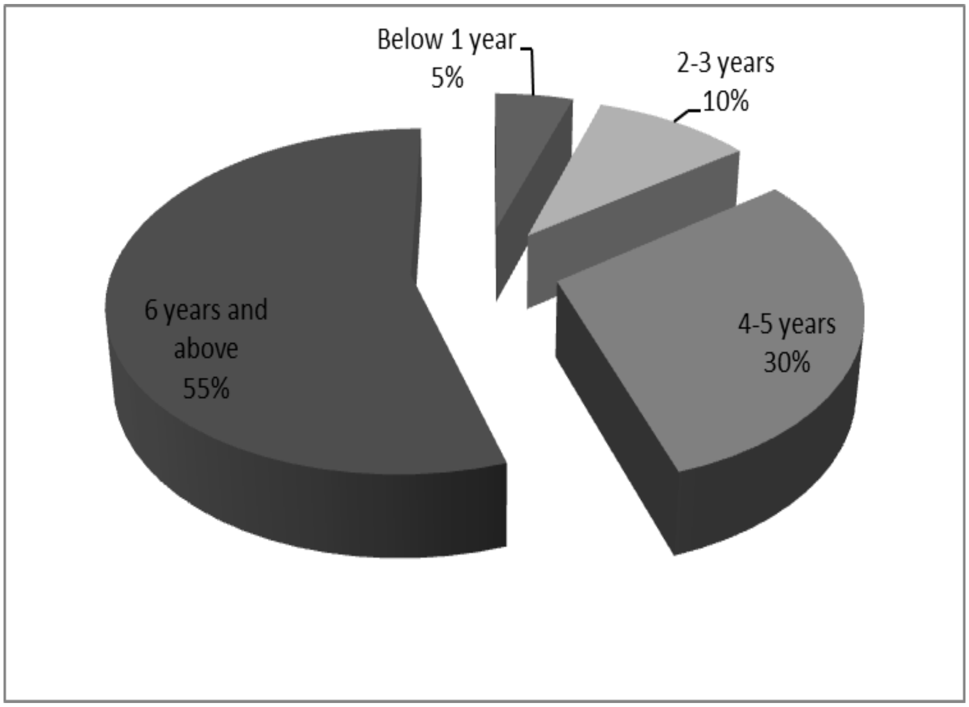


From the findings in Figure 4.6, 30% of the respondents indicate that their organizations had more than 200 employees, 15% indicated 176-200 and 151-175 employees respectively, 10% indicated 126-150 and 101-125 respectively. Further 8% of the respondents indicated 76-100 employees, 6% indicated 56-75 employees, 5% indicated 26-55 respondents while 1% indicated 0-25 employees. This depicts that majority of the respondents indicated their organizations had more than 200 employees.

4.2.6. Length of Operation of the Organization

The respondents were requested to state the length of operation of their organization. The findings were as shown in Figure 4.7

Figure 4.7.Length of Operation of the Organization

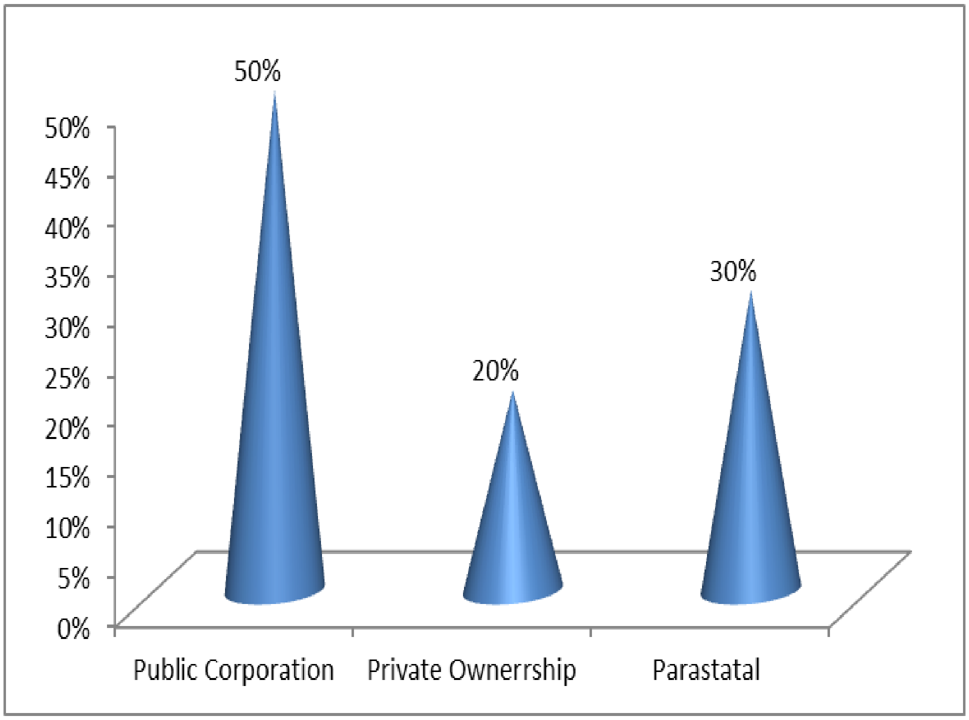


From the findings in Figure 4.7, 55% of the respondents indicated that their organization have been in operation for more than 6 years, 30% indicated between 4-5 years, 10% indicated 2-3 years while 5% indicated below 1 year. This shows that most organizations have been in operation for more than 6 years.

4.2.7. Ownership of the Organization

The respondents were kindly requested to indicate the ownership of their organization. The findings were shown in Figure 4.8

Figure 4.8. Ownership of the Organization

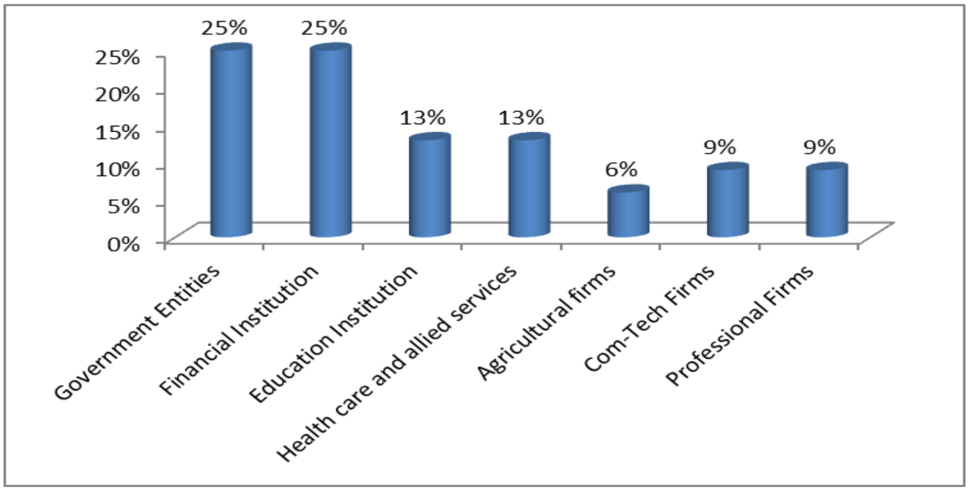


From the findings in Figure 4.8, 50% of the respondents indicated their organizations were public owned corporation, 30% indicated parastatal while 20% indicated they were private owned. This depicts that most of the organizations were public owned corporation.

4.2.8. Sectors to which the Organizations belong

The respondents were requested to indicate the sector their organizations belonged to. The findings were shown in Figure 4.9

Figure 4.9. Sectors to which the Organizations belong



From the findings in Figure 4.9, 25% of the respondents indicated that their organization belong to government entities and financial institutions sectors respectively, 13% indicated educational institutions and Health care and allied services respectively. Further 9% of the respondents indicated that their organizations belong to Communication and technology firms and Professional firms sectors respectively while 6% indicated agricultural firms. This depicts that most organizations belong to government entities and financial institutions sectors.

4.3. Extent to which the Organization has used the Security Threat Mitigation Measures

The respondents were requested to indicate the extent to which the organization has used the security threat mitigation measures. The responses were placed on a five Likert scale ranging from 1 (To a no extent) to 5 (To a very great extent). The findings were as shown in Table 4.2

Table 4.2. Extent to which the Organization has used the Security Threat Mitigation Measures

Security measure	**Mean**	**Std Dev.**
Use of two factor authentication for access to data center	4.14	0.223
Performance of regular integrity checks	3.99	0.334
Third party security validation	4.09	0.186
Controlled access to data storage centers	4.12	0.224
Destruction of data upon authorization by the client	3.88	0.124
Use of firewalls protect servers	3.79	0.345
Existence of threats detection mechanisms	4.02	0.228
Existence of data recovery mechanisms	4.04	0.174
Encrypted communication between providers and users	3.68	0.248
Secure isolation of customer data	3.58	0.388
Regular data back-ups	3.92	0.313
Host-based intrusion detection	3.72	0.129
Defining and implementing data security in the life cycle of customer data	4.08	0.222
Strict adherence to minimum security standards in the development of applications	3.66	0.382
Robust infrastructure with adequate resistance to damage	3.82	0.143
Use of antiviruses	4.01	0.168

From the findings in Table 4.2, the respondents agreed that use of two factor authentication for access to data center was the highly used measure (mean=4.14), followed by controlled access to data storage centers (mean=4.12), third party security validation (mean=4.09), defining and implementing data security in the life cycle of customer data (mean=4.08). In addition, respondents agreed that existence of data recovery mechanisms was also used (mean=4.04), Existence of threats detection mechanisms (mean=4.02), Use of antiviruses (4.01), performance of regular integrity checks (mean=3.99), regular data back-ups (mean=3.92), destruction of data upon authorization by the client (mean=3.88). The respondents further agreed that robust infrastructure with adequate resistance to damage was a measure that was also used (mean=3.82), use of firewalls protect servers (mean=3.79), host-based intrusion detection (mean=3.72), encrypted communication between providers and users (mean=3.68), strict adherence to minimum security standards in the development of applications (mean=3.66) and secure isolation of customer data (mean=3.58). This implies that use of two factor authentication for access to data center was the highly used measure in information security.

4.4. Relationship between Security Measures and Security Levels

There exists a direct relationship between security measures in place and security levels of a system. Security measures enhance the level of security of information and thus make it free from invasion by various information threats.

4.4.1. Extent of Contribution of Security Measures to the Security Level in the Organization

The respondents were requested to indicate the extent of contribution of security measures to the security level in the organization. The responses were placed on a five Likert scale ranging from 1 (To a no extent) to 5 (To a very great extent). The findings were as shown in Table 4.3

Table 4.3. Extent of Contribution of Security Measures to the Security Level in the Organization

Security measure	**Mean**	**Std Dev.**
Use of two factor authentication for access to data center	4.22	0.356
Performance of regular integrity checks	4.04	0.163
Third party security validation	4.18	0.327
Controlled access to data storage centers	4.20	0.180
Destruction of data upon authorization by the client	3.95	0.241
Use of firewalls protect servers	3.86	0.289
Existence of threats detection mechanisms	4.12	0.366
Existence of data recovery mechanisms	4.14	0.211
Encrypted communication between providers and users	3.79	0.387
Secure isolation of customer data	3.69	0.238
Regular data back-ups	4.02	0.122
Host-based intrusion detection	3.82	0.345
Defining and implementing data security in the life cycle of customer data	4.16	0.126
Strict adherence to minimum security standards in the development of applications	3.72	0.172
Robust infrastructure with adequate resistance to damage	3.89	0.221
Use of antiviruses	4.08	0.338

From the findings in Table 4.3, the respondents agreed that use of two factor authentication for access to data center was the highly contributed to the security level (mean=4.22), followed by controlled access to data storage centers (mean=4.20), third party security validation (mean=4.18), defining and implementing data security in the life cycle of customer data (mean=4.16). In addition, respondents agreed that existence of data recovery mechanisms also contributed to security levels (mean=4.14), existence of threats detection mechanisms (mean=4.12), Use of antiviruses (4.08), performance of regular integrity checks (mean=4.04), regular data back-ups (mean=4.02), destruction of data upon authorization by the client (mean=3.95).

The respondents further agreed that robust infrastructure with adequate resistance to damage contributed to security level (mean=3.89), use of firewalls protect servers (mean=3.86), host-based intrusion detection (mean=3.82), encrypted communication between providers and users (mean=3.79), strict adherence to minimum security standards in the development of applications (mean=3.72) and secure isolation of customer data (mean=3.69). This implies that use of two factor authentication for access to data center was the highly contributed to the security level.

4.4.2. Extent to which Security Levels have been affected by the Mitigating Measures

The respondents were requested to indicate the extent to which security levels have been affected by the mitigating measures. The responses were placed on a five Likert scale ranging from 1 (To a no extent) to 5 (To a very great extent). The findings were as shown in Table 4.4.

Table 4.4. Extent to Which Security Levels have been affected by the Mitigating Measures

Security measure	**Mean**	**Std Dev.**
Information access has been made easier	3.67	0.335
There has been significant decreases in malware	4.09	0.222
Durability of information applications has improved	4.02	0.358
Customers data has been secured with appropriate passwords	4.01	0.256
Hacking incidences have reduced	3.89	0.145
Extent of customers information loss has reduced	3.70	0.138
Data has been protected from manifestation of viruses	4.14	0.332
Intrusion by the web hackers has been prevented	3.69	0.123
There has been a reduction of information corruption	3.54	0.331
Detection of a threat have been detected before they damage the whole information system	3.99	0.186

From the findings in Table 4.4, the respondents indicated that data has been protected from manifestation of viruses (mean=4.14), followed by there has been significant decreases in malware (mean=4.09), durability of information applications has improved (mean=4.02), customers data has been secured with appropriate passwords (mean=4.01). The respondents further agreed that detection of a threat have been detected before they damage the whole information system (mean=3.99), hacking incidences have reduced (mean=3.86), extent of customers information loss has reduced (mean=3.70). In addition the respondents agreed that intrusion by the web hackers has been prevented (mean=3.69), information access has been made easier (mean=3.67), and there has been a reduction of information corruption (mean=3.54). This depicts that data security levels have improved in that data has been protected from manifestation of viruses.

4.5 Regression Analysis

The researcher further conducted a multiple regression analysis in order to test the threats mitigation measures and security of cloud based enterprise resource planning system in Kenya. Statistical package for social sciences (SPSS) was used to code, enter and compute the measurements of the multiple regressions for the study. Coefficient of determination explains the extent to which changes in the dependent variable can be explained by the change in the independent variables or the percentage of variation in the dependent variable (financial performance) that is explained by all the four independent variables (size of the bank, product innovation, process innovation and market innovation).

4.5.1 Model Summary

Table 4.5. Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	0.857	0.735	0.689	0.5273

The coefficient of determination (R Square) is used to test the goodness-of-fit of the model. That is, R Square measures the proportion or percentage of the total variation in the dependent variable explained by the independent variable. The value of R Square lie between 0 and 1 and if R Square value is 1 there is a perfect fit while R Square value 0 indicates that there is no relationship between dependent and independent variables. The 10 independent variables that were studied, explain only 73.5% of the security of cloud based enterprise resource planning system as represented by the R^2. This therefore means that other threat mitigation measures affecting security of cloud based enterprise resource planning system not studied in this research add up to 26.5%.

4.5.2. ANOVA Results

Table 4.6. ANOVA of the Regression

Model		**Sum of Squares**	**df**	**Mean Square**	**F**	**Sig.**
1	Regression	2.534	3	1.267	9.475	.0031
	Residual	9.307	50	2.327		
	Total	**11.841**	**53**			

The significance value is 0.031which is less than 0.05 thus the model is statistically significance in predicting how the threats mitigation measures (Controlled access to data storage centers, third party security validation, Existence of data recovery mechanisms, Existence of threats detection mechanisms, Performance of regular integrity checks, Regular data back-ups, Host-based intrusion detection, Authentication procedures, Use of Firewalls, Secure isolation of customer data) affect the security of cloud based enterprise resource planning system. The F critical at 5% level of significance was 3.23. Since F calculated is greater than the F critical (value = 9.475), this shows that the overall model was significant.

4.5.3. Coefficient of Determination

Table 4. 7. Coefficient of Determination

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	1.127	0.2235		5.132	0.000
	Controlled access to data storage centers	0.752	0.2050	0.1032	3.668	.000
	Third party security validation	0.652	0.1032	0.1425	6.318	.000
	Existence of data recovery	0.587	0.1125	0.1178	4.844	.000
	Existence of threats detection	0.545	0.0937	0.0937	5.816	.000
	Performance of regular integrity	0.525	0.1178	0.2634	4.457	.000
	Regular data back-ups	0.509	0.1532	0.0543	3.322	.000
	Host-based intrusion detection	0.487	0.1123	0.1254	4.336	.000
	Authentication procedures	0.469	0.1237	0.0987	3.791	.000
	Use of Firewalls	0.457	0.1356	0.2786	3.370	.000
	Secure isolation of customer data	0.445	0.1450	0.1687	3.069	.000

Multiple regression analysis was conducted as to determine the threats mitigation measures and security of cloud based enterprise resource planning system in Kenya and the ten variables. As per the SPSS generated table below, regression equation

$(Y = \beta_0 + \beta_1X_1 + \beta_2X_2 + \beta_3X_3 + \beta_4X_4 + \beta_5X_5 + \beta_6X_6 + \beta_7X_7 + \beta_8X_8 + \beta_9X_9 + \beta_{10}X_{10} + e)$ becomes:

$(Y = 1.127 + 0.752X_1 + 0.652X_2 + 0.587X_3 + 0.545X_4 + 0.525X_5 + 0.509X_6 + 0.487X_7 + 0.469X_8 + 0.457X_9 + 0.445X_{10} + e)$

According to the regression equation established, taking all factors into account (Controlled access to data storage centers, third party security validation, Existence of data recovery mechanisms, Existence of threats detection mechanisms, Performance of regular integrity checks, Regular data back-ups, Host-based intrusion detection, Authentication procedures, Use of Firewalls, Secure isolation of customer data) constant at zero, the security of cloud based enterprise resource planning system will be 1.127. The data findings analyzed also showed that taking all other independent variables at zero, a unit increase in controlled access to data storage centers will lead to a 0.752 increase in the security of cloud based enterprise resource planning system.

A unit increase in Third party security validation will lead to a 0.652 increase in the security of cloud based enterprise resource planning system, a unit increase in Existence of data recovery will lead to a 0.587 increase in the security of cloud based enterprise resource planning system; a unit increase in Existence of threats detection will lead to a 0.545 increase in the security of cloud based enterprise resource planning system; a unit increase in Performance of regular integrity will lead to a 0.525 increase in the security of cloud based enterprise resource planning system; a unit increase in Regular data back-ups will lead to a 0.509 increase in the security of cloud based enterprise resource planning system; a unit increase in Host-based intrusion detection will lead to a 0.487 increase in the security of cloud based enterprise resource planning system; a unit increase in Authentication procedures will lead to a 0.469 increase in the security of cloud based enterprise resource planning system; a unit increase in Use of Firewalls will lead to a 0.457 increase in the security of cloud based enterprise resource planning system; a unit increase in Secure isolation of customer data will lead to a 0.445 increase in the security of cloud based enterprise resource planning system.

This infers that Controlled access to data storage centers contributes the most to the security of cloud based enterprise resource planning system followed by Third party security validation. At 5% level of significance and 95% level of confidence, Controlled access to data storage centers, third party security validation, Existence of data recovery mechanisms, Existence of threats detection mechanisms, Performance of regular integrity checks, Regular data back-ups, Host-based intrusion detection, Authentication procedures, Use of Firewalls, Secure isolation of customer data were all significant measures on the security of cloud based enterprise resource planning System.

4.6. Discussion of Findings

The study found that use of two factor authentication for access to data center was the highly used measure in information security. The study also found that use of two factor authentication for access to data center was the highly contributed to the security level. This concurs with a study done by Almorsy, Grundy and Mueller, (2010), who asserted that all organizations and people are driven by the need to have sensitive information about them protected from leakage, unauthorized access/alteration, loss or destruction by the use of measures such as use of two factor authentication for access to data center was the highly used measure in information security.

The study also found that data security levels have improved in that data has been protected from manifestation of viruses. This tends to agree with a study by Davenport (2013), who asserted that ERP systems provide seamless integration of all information flowing through a company's departments. With the seamless integration of information within institutions, managers are able to overcome threats that are emanating from incompatible systems and inconsistent operating practices. Acquisition of these systems may be through commercial off-the-shelf systems or custom designed systems in line with an organizational needs.

CHAPTER V: SUMMARY, CONCLUSION AND RECOMMENDATIONS

5.1 Introduction

This chapter presents summary, conclusion and recommendations on the threats mitigation measures and security of cloud based enterprise resource planning system in Kenya.

5.2 Summary of Findings

The study found that that majority of the respondents were between the age of 26-30 years. The study also found that majority of the respondents were males and that majority of the respondents were IT managers. The study also found that majority of the respondents had worked in the organization for a period between 6-10 years.

The study also indicated that majority of the respondents indicated their organizations had more than 200 employees. Further the study found that most organizations have been in operation for more than 6 years. Finally the study found that most of the organizations were public owned corporation and that most organizations belong to government entities and financial institutions sectors.

The study found that use of two factor authentication for access to data center was the highly used measure in information security. The study also found that use of two factor authentication for access to data center was the highly contributed to the security level. The study also found that data security levels have improved in that data has been protected from manifestation of viruses.

5.3. Conclusion

The study concluded that use of two factor authentication for access to data center was the highly used measure in information security. The study also concluded that use of two factor authentication for access to data center was the highly contributed to the security level. The study also concluded that data security levels have improved in that data has been protected from manifestation of viruses. Finally, from the regression analysis, the study concluded that controlled access to data storage centers contributes the most to the security of cloud based enterprise resource planning system followed by third party security validation.

At 5% level of significance and 95% level of confidence, controlled access to data storage centers, third party security validation, existence of data recovery mechanisms, existence of threats detection mechanisms, performance of regular integrity checks, regular data back-ups, host-based intrusion detection, authentication procedures, use of firewalls, secure isolation of customer data were all significant measures on the security of cloud based enterprise resource planning system.

5.4. Recommendations

From the findings of the study the following recommendations were made:

1. Despite the wide popularity of cloud computing internationally, the study recommends that there are prior issues that need to be addresses with the technology itself before most clients can embrace it fully

2. The study also recommend more to be done to establish the compatibility between cloud solutions with enterprises' legacy systems and business needs, as well as the impact of trying or using cloud solutions on organizational culture, staff skills, and work practices.

3. The study also recommends that cloud computing adoption processes should be well documented and more attention should be directed at this area to explore the challenges faced in each stage of the process.

5.5. Limitations of the Study

The findings of this study can only be directly applicable to organizations with cloud computing and ERP in Kenya hence may not be directly applicable to any other organization unless it has integrated the cloud ERP in its systems. It is also important to note that the relevance of this information is limited to the duration within which the study was carried out. Changes are bound to occur that may transform the way activities are carried out in the ERP based organizations thus making significant changes in future

5.6. Recommendation for Further Research

Technology plays a role in enhancing information security. Therefore, research should be carried out on ways in which this could be used to enhance security of data and customer's information. A study should also be done on cloud computing in all organization in Kenya to determine the level of preparedness in relation to ERP.

In addition, the researcher conducted a study of the organizations with ERP and cloud computing only and therefore recommends that for a more generalized conclusion to be made to improve the current ERP operations and cloud computing and how they impact on information security. Repeat surveys, will also offer a distinct advantage as they enable us to capture the net effect changes. By repeating the survey at a different time and asking fairly similar questions, it enables us to collect information that can easily be compared.

REFERENCES

Al-Fawaz M., Zahran F., & Tillal G.,(2008). Investigating the Link between Enterprise Resource Planning . *European Journal of Business and Management Vol.5, No.13,*, 93-98.

Almorsy A., Grundy H. & Mueller A., (2010). 'Internal audit in Italian Organizations', *Managerial Auditing Journal,* 21 (3), pp. 275-292.

Verville G., & Halingten R. (2003). An approach to a cloud computing network. Proceedings of the First International Conference on the Applications of Digital Information and Web Technologies, 113-118.

Basoglu N., Daim T., & Kerimoglu O., (2007) Organization Adoption of Enterprise Resource Planning Systems: A Conceptual Framework, *Journal of High Technology Management Research* 18(1) 73-97.

Boss, G., Malladi, P., Quan, D., Legregni, L., & Hall, H., (2007). Cloud Computing. *ww.ibm.com/developer works/web sphere/zones/hipods/. Retrieved on 20th May, 2010.*

Colwill, C. (2009). Human factors in information security: The insider threat – Who can you trust these days? Information Security Technical Report, 14(4), 186-196.

Cornford E. & Pollock Z. (2004), "Cloud computing and the business consequences of ERP use," *International Journal of Computer Applications*, pp. 28-31.

CSO Magazine. (2011). 2011 Cyber security watch survey. CSO Magazine. Retrieved from *https://www.cert.org/insider-threat/research/cybersecurity-watch-survey.cfm.*

Daniel E. (2008). *Complexity Is the Enemy, IEEE Security and Privacy*. Vol. 6, No. 6.

Davenport, H., (2003). *Enterprise Systems in Universities*: Panacea or Can of Worms? JISC: info Net Publication. North Umbria University.

Davenport, H., (2011). Critical Success Factors for Enterprise Resource Planning Implementation and Upgrade; *Journal of Computer Information Systems – Special Issue; Lincoln: Nebraska University*.

David, B., (2009). Top Five Cloud Computing Security Issues, Computer Weekly *http://www.computerweekly.com/Articles/2010/01/12/235782/Topfive-cloud-computingsecurity-issues.htm>*.

Delone, F., & McLean N., (2003). *Information system: analysing the impact.* Integrated Manufacturing Systems, Vol. 12 Iss 2, pp. 103 - 113.

Foster et al., (2008). Guest Editorial: the challenge of managing information security. *International Journal of Information Management*. Volume 24. pp 3 – 4.

Sullivan, H., & Bozeman, K., (2010). "Challenges involved in implementation of ERP on demand solution: Cloud computing," *International Journal of Computer Science Issues* (IJCSI), pp. 9-481.

Ferrell, M., (2003). Cloud Computing and Grid Computing 360 Degrees Compared. In: Grid Computing Environments Workshop (GCE'08). *doi:10.1109/GCE.2008.4738445.*

Fers, H., (2010). "The adoption of software-as-a-service (SaaS): ranking the determinants". *Journal of Enterprise Information Management, Vol. 28 Iss 3,* pp. 400 - 422.

Fishbein, G., & Ajzen, B., (1975). '*Corporate governance, internal audit and environmental audit - the performance tools in Romanian companies'*, Accounting and Management Information Systems, 11(1), pp. 112-130.

Hyvonen, V., (2003). *A theoretical extension of the technology acceptance model*: Four longitudinal field studies. Management Science, 46(2), 186–204.

Jadeja, A., & Modi, M., (2012), Decision criteria in the adoption of Edi. In Proceedings of 14th Annual International Conference on Information Systems Orlando, Florida, December, (pp. 365– 376).

Kahigu, N., (2004), A view of cloud computing. Communication of ACM, 53(4), 50–58.

Kebs, J., (2012). A meta-analysis of the technology acceptance model. Information & Management, 43(6), 740–755.

Khajeh-Hosseini, A., Sommerville, I., & Sriram, I., (2010b). Research Challenges for Enterprise Cloud Computing. Submitted to the 1st ACM Symposium on Cloud Computing, SOCC 2010.

Kim, A., (2009). Research Challenges for Enterprise Cloud Computing. Submitted to the 1st ACM Symposium on Cloud Computing, SOCC 2010.

King, H., & He, B., (2006). Managerial Issues of Enterprise Resource Planning Systems, McGraw Hill, Taiwan.

Kituku, K. M. (2012). Adoption of cloud computing in kenya by firms listed in the nairobi stock exchange. *A management research project, University of Nairobi*.

Kitur, F., (2011). Cloud Migration: A Case Study of Migrating an Enterprise IT System to IaaS. Submitted to IEEE CLOUD 2010.

Klein, J., (2003). Cloud Migration: A Case Study of Migrating an Enterprise IT System to IaaS. Submitted to IEEE CLOUD 2010.

Kotb, A. & Roberts, C. (2011) 'the impact of E-business on the audit process: an investigation of the factors leading to change', *International Journal of Auditing*, 15, pp. 150-75.

Kshetri, H., (2012). 'Auditing in enterprise system environment: a synthesis', *Journal of Enterprise Information Management,* 24 (6), pp. 494-519.

Lelei, J., (2008). ICT as a strategic tool in microfinance institutions in Kenya. *Electronic Commerce Research and Applications,* 8(3), 130–141.

Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J., & Ghalsasi, A. (2011). Cloud Computing-The business Perspective. *Decision Support Systems,* 51, 176-189.

Mavodza, G., (2012). 'The role of internal auditors in ERP-Based organizations', *Journal of Accounting and Organizational Change,* 5 (4), pp. 514-526.

McLaughlin, G., (2008). *Software as a service inflection point: Using cloud computing to achieve business agility.* New York: Global Authors Publishers.

Medlin, K., (2001). Critical Factors for Successful Implementation of Enterprise Systems. *Business Process Management,* 7(3).

Mohamed, A., & Pillutla, M. A., (2014). Collaboration-Based Cloud Computing Security Management Framework. *IEEE International Conference on Cloud Computing (CLOUD 2011).* Washington DC, USA on 4 July – 9 July, 2011, IEEE.

Madden, A., Ellen, J., & Ajzen, D., 1992; Yi et al., 2005). Enterprise resource planning, operations and management. *International Journal of Operations & Production Management, Vol. 33 Iss 8,* pp. 1075 - 1104 .

Mugenda, A.G. (2003). *Social Science Research.* Nairobi: Acts Press.

Mugenda, O. M & Mugenda, A.G (2008). *Research methods, Quantitative and Qualitative approach,* Nairobi.

Musyoka, S., (2004). Electronic commerce adoption: An empirical study of small and medium US businesses. *Information and Management*, 42(1), 197–226.

Lee, Y., Li, K., Yen, & Huang, Y., (2010). Reflections on computer-related risks. *Communications of the TAM,* 51(1), 78-80.

Nyandiere et al (2012), Critical Factors for Successful ERP Implementation: Exploratory Findings from Four Case Studies. *Communications of the ACM*, 56(6).

Omwansa, R., Waema, A., & Omwenga, F., (2015),*Cloud computing in Kenya: A baseline survey*. Nairobi.

Pollock, D., (2004). *"ERP systems and the university as a "unique" organization",* Information Technology & People, Vol. 17 Iss: 1, pp.31 – 52.

Robinson, M., (2009). Cloud computing: A new business paradigm for biomedical information sharing. *Journal of Biomedical Informatics.*

Rogers, E. M. (2003). *Diffusion of innovations* (4th ed.). NJ, New York: Free Press.

Sabahi, B., (2011). 'ERP systems and Internal Audit', *Issues in Information Systems, XL* (2), pp.578-586.

Schubert, P. (2011). Cloud Computing for Standard ERP Systems: Reference Framework and Research Agenda, *Available at http://academia.edu/Documents/in/Enterprise_Systems.*

Sofa, G., Dori, N.,, 2002; & Sedeta, A., (2004). Let me in the cloud: analysis of the benefit and risk assessment of cloud platform. *Journal of Financial Crime, Iss 1* , pp. 6 - 24.

Steele, S., & Wargo, C. (2007). An introduction to insider threat management. Information Systems Security, 16(1), 23-33.

Sultan, H., (2011). User acceptance of information technology: Toward a unified view. *MIS Quarterly,* 27(3), 425–478.

Vishal, S., (2009). Factors influencing the adoption of internet banking: An integration of TAM and TPB with perceived risk and perceived benefit.

Widup, S. (2010). The leaking vault–Five years of data breaches. Digital Forensics Association.

Yetton, A., & Sharma, V., (2003). Enterprise Resource Planning: Implementation procedures and Critical success factors; *European Journal of Operational research*; 146 (2): 241 –257.

APPENDIX I: QUESTIONNAIRE

SECTION A: GENERAL INFORMATION

1. Name of the respondent (optional)

   ____

2. Age of respondent

   21- 25 years [ ]   26 – 30 years [ ]

   31 – 35 years [ ]   36 – 40 years [ ]

   Over 40 years [ ]

3. Gender

   Male [ ]   Female [ ]

4. Position in the organization

   IT Manager [ ]   Technician [ ]

   IT Engineer [ ]   Other [ ]

   Specify if other ……………………………………………………….

5. How long have you worked for the organization

   Less than 1 year [ ]   1 – 5 year [ ]

   6– 10 years [ ]   Over 10 years [ ]

6. How many employees does your organization have?

   0 – 25 [ ]   26 – 50 [ ]

51– 75 [ ] 76 – 100 [ ]

101-125 [ ] 126-150 [ ]

151-175 [ ] 176-200 [ ]

Over 200 [ ]

7. How long has your organization been operational?

   Below 1 year [ ]

   2-3 years [ ]

   4-5 years [ ]

   6 years and above [ ]

8. What is the ownership of your organization?

   Public corporation [ ]

   Private ownership [ ]

   Parastatal [ ]

9. In which of the sectors below does your organization fall? Please tick [√] only one.

   Government entities..[ ]

   Financial institutions..[ ]

   Educational institutions... ..[ ]

   Health care and allied services.....................................[ ]

   Agriculture firms..[ ]

   Communication and technology firms..........................[ ]

   Professional firms...[ ]

Give a brief description of the operations of your organization

……………………………………………………………………………………………...

SECTION B: SECURITY MEASURES

10. Indicate the extent to which the organization has used each of the following security threat mitigation measures in the organization. Use a scale where 1- To no extent, 2- To low extent, 3- To moderate extent, 4- To great extent and 5-To very great extent

Statements	No extent	Low extent	Moderate extent	Great extent	Very great extent
Use of two factor authentication for access to data center					
Performance of regular integrity checks					
Third party security validation					
Controlled access to data storage centers					
Destruction of data upon authorization by the client					
Use of firewalls protect servers					
Existence of threats detection mechanisms					
Existence of data recovery mechanisms					
Encrypted communication between providers and users					
Secure isolation of customer data					
Regular data back-ups					
Host-based intrusion detection					
Defining and implementing data security in the life cycle of customer data					
Strict adherence to minimum security standards in the development of applications					
Robust infrastructure with adequate resistance to damage					
Use of antiviruses					
Other (specify and rate accordingly)					

SECTION C: RELATIONSHIP BETWEEN SECURITY MEASURES AND SECURITY LEVELS

11. State the extent of contribution of each of the following security measures to the security level in your organization. Use a scale where 1- To no extent, 2- To low extent, 3- To moderate extent, 4- To great extent and 5-To very great extent

Statements	No extent	Low extent	Moderate extent	Great extent	Very great extent
Use of two factor authentication for access to data center					
Performance of regular integrity checks					
Third party security validation					
Controlled access to data storage centers					
Destruction of data upon authorization by the client					
Use of firewalls protect servers					
Existence of threats detection mechanisms					
Existence of data recovery mechanisms					
Encrypted communication between providers and users					
Secure isolation of customer data					
Regular data back-ups					
Host-based intrusion detection					
Defining and implementing data security in the life cycle of customer data					
Strict adherence to minimum security standards in the development of applications					
Robust infrastructure with adequate resistance to damage					
Use of antiviruses					
Other (specify and rate accordingly)					

12. Indicate the extent to which the security levels in your organization have been affected by the mitigating measures. Use a scale where 1- To no extent, 2- To low extent, 3- To moderate extent, 4- To great extent and 5-To very great extent.

Statement	No extent	Low extent	Moderate extent	Great extent	Very great extent
Information access has been made easier					
There has been significant decreases in malware					
Durability of information applications has improved					
Customers data has been secured with appropriate passwords					
Hacking incidences have reduced					
Extent of customers information loss has reduced					
Data has been protected from manifestation of viruses					
Intrusion by the web hackers has been prevented					
There has been a reduction of information corruption					
Detection of a threat have been detected before they damage the whole information system					

THANK YOU FOR YOUR PARTICIPATION