UNIVERSITY OF NAIROBI
COLLEGE OF BIOLOGICAL AND PHYSICAL SCIENCES
SCHOOL OF COMPUTING AND INFORMATICS

MASTER OF SCIENCE IN INFORMATION SYSTEMS
RESEARCH PROJECT

TOPIC:

ENTERPRISE INFORMATION SECURITY ARCHITECTURE (EISA)

TITLE:

A Methodology for Adoption of an Enterprise Information Security Architecture Model: A Case Study of Major Companies in the Oil and Gas Industry in Kenya.

DANIEL K. SIGEI
P56/70452/2007

DECLARATION

STUDENT

I, the undersigned, declare that this project is my original work and that it has not been presented in any other university or institution for academic credit.

NAME: **REG:**

Signature ..... Date 2 : 11 : 2012 .....

SUPERVISOR

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

Signed ..... Date 7/11/2012 .....

DEDICATION

This Master of Science research project is dedicated to my late father Mr. Wilson Kipsigei Arap Chebochok, my dear mother Anne and my beloved wife Yano and children Tony, Charlie, Olivs and Chemu.

ACKNOWLEDGEMENT

I acknowledge the power of God, the Almighty and the provider of knowledge for enabling me to complete this course in his own appointed time.

Most important, I sincerely wish to acknowledge the support from my supervisor Andrew Mwaura, and panel members Robert Oboko and Evans Miriti without whom I could not have gone this far with my project work.

I would like to thank C A. Moturi whose encouragement in my entire academic life was significant.

To all my lecturers at the University of Nairobi, School of Computing and Informatics, who contributed in one way or another in quenching my thirst for knowledge I owe you my sincere gratitude.

I salute the dedication of Jona Akello Owitti, my mentor, for encouraging me to continue University Education in the field of computer science and information systems.

I owe a great deal of gratitude to all my immediate and extended family members for their unfailing moral support throughout my period of study and for understanding and appreciating the demands of the course in terms of time and resources.

I cannot forget my early teachers, colleagues, and classmates who influenced me positively in my life and were a source of inspiration throughout my study and for assisting me in sourcing for information and materials for this project. To you all, God bless.

ABSTRACT

The purpose of this study is to investigate the adoption and assimilation of Enterprise Information Security Architecture (EISA) as an administrative innovation within the Oil and Gas Industry in Kenya. EISA is a subset of Enterprise Architecture (EA), focusing on information security in the enterprise. Several EISA frameworks have been developed and have gained acceptance, particularly in the developed world. However, their adoption rate in Kenya remains undocumented, despite Kenya's relatively well developed ICT infrastructure as compared to other countries within the East African Region. In Kenya, the context in which this study takes place, no literature exists on adoption and assimilation of EISA either as an administrative innovation or technological innovation. Studies show that information security managers, including those in Kenya, have been searching for rationalized security practices to manage risks, preserve the confidentiality, integrity and availability of information and ensure business continuity in their organizations. This is a natural response to the increasing external threats and potential leakage of information. Such efforts can be viewed, conceptually, as a form of administrative innovation as it triggers organizational change. Technological innovation focuses on developments in security technologies whereas EISA fits with the philosophy of administrative innovation. If security were to be treated as a technological innovation, research into adoption and assimilation of EISA would inevitably regarded incorrectly as part of ICT security. This study used administrative adoption models and hypotheses to test the factors that influence the assimilation and adoption of EISA frameworks in Kenya. The results indicate that supervisory authority can play a significant role in stimulating and enforcing the adoption and assimilation of information security architecture as a management practice. This can offer some encouraging evidence for regulators to evaluate the effectiveness of rules and regulations in the area of Information security architecture.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER ONE:
INTRODUCTION

1.1 Background of the study

Information is one of the most important assets in an enterprise and should be appropriately protected. Information Security is the combining of systems, operations and internal controls to ensure the confidentiality, integrity, and availability of data in an organization. Given the wide acceptance and use of information technology (IT), users can now operate most IT solutions on their own, directly and with limited help of IT specialists. As a result of rapid advances in IT, information security is facing unprecedented challenges, and effective information security management is one of the major concerns.

Although there is plenty of security technology research, surprisingly few information security management studies are found in the literature. It wasn't until 1995, when the British Standard Institution (BSI) established BS7799-1, "Information Security Management – Part I: Code of Practice for Information Security Management", that a more complete management framework for information security emerged.

While information security has always been a concern, it has become even more critical with the proliferation of the Internet. Whereas in the past enterprises were concerned only with protecting the flow of information within the business, today they must consider the threat from outside – from attacks on the security of the corporate Intranet, for instance, or electronic data interchange (EDI) between the enterprise, clients and suppliers.

Today's enterprises are doing a good job to secure their information, but they are the exception rather than the norm. The majority are grappling with basic information security issues, and yet information security principles of confidentiality, integrity and availability are often touted as critical to achieving business goals. The big question is: why is this? One reason is that most businesses are focused on delivering

a strong short-term performance, which conflicts with information security initiatives, as these usually have a less direct return on investment, and are competing for scarce resources with other programs that promise quick return and immediate benefits. Another reason is that the majority of enterprises that have tried to implement information security in their organization have taken the wrong approach e.g. assigning the information security implementation to a single individual or department. This approach ultimately fails because security has an important property that most people know about but few pay any real heed to it: it is like a chain link that is made of many links.

Since almost every enterprise has a system of information security or protection, perhaps we should ask the question: how do enterprises adopt and assimilate these systems? Looking at recent developments, it is not in doubt that Kenyan managers are actively searching for rationalized security management processes to manage risks, and to preserve the confidentiality, integrity and availability of information. This study views such efforts as a form of administrative innovation. According to Hsu et al (2009) "administrative innovations have been viewed in this light before". An innovation is "any idea, practice, or material artifact perceived to be new by the unit of adoption" (Zaltman et al.1973, p.158). Hsu et al (2009) "administrative innovation is synonymous with organization change, however major or minor it may appear to be. It is thus conceptually related to change management ". A great effort is required to ensure administrative innovations form an integral part of an organization's business process. Researchers in a variety of disciplines have discussed the conditions that facilitate or hinder the adoption and assimilation of organizational innovations (Hsu et al 2009). However, there has been little focus on both adoption and assimilation in a single study, or indeed on other forms of innovations with an administrative core (Teece 1980, Westphal et all. 1997).

A more detailed understanding of information security architecture as an administrative innovation is desirable as it will address the research gap that exists in Kenya. Moreover, the outcome will be relevant because there is no model to depict

how organizations in Kenya adopt and assimilate administrative innovations in response to institutional requirements.

1.2 Statement of the Problem

The pervasive lack of information security may be attributed to the notion that building security into information systems is a matter of referring to a checklist and applying the appropriate measures to plug the holes. Such a notion is clearly misplaced. Security has an important property that most people know about but few pay any real heed to it: it is like a chain, made up of many links, and the strength and suitability of the chain is only as good as that of its weakest link. At worst, if one link is missing, the rest of chain has limited or no value. A key pitfall of the notion that focuses on the chain link is that it does not test that the links actually fit together to form a secure chain. The chain is a reasonably good analogy, but the problem in building security into information systems is actually much bigger. Imagine a checklist that has the following items: engine block; pistons; piston rings; piston rods, bearings, valves; cam shaft, wheels, chassis, body, seats, steering wheel, gearbox, etc. Suppose that this list comprehensively itemizes every single component that would be needed to build a car. If you go through the checklist and make sure that you have all of these components, does it mean that you have a car?

A car is a good example of a complex system. It has many sub-systems, which in turn have sub-systems, and eventually a very large number of components. Designing and building a car needs a 'systems-engineering' approach. Examples of key questions not addressed by the checklist approach are: Do you understand the requirements? Do you have a design philosophy? Do you have all of the components? Do these components work together? Do they form an integrated system? Does the system run smoothly? Are you assured that it is properly assembled? Is the system properly tuned? Do you operate the system correctly? Do you maintain the system? The analogy of the car as a complex machine that needs a holistic architectural design is much more powerful than the idea of a chain. Security architecture is more like the car, not the chain.

The primary need in this study is for a simple structured and practical methodology for adoption and assimilation of information security architecture to support the evolving IT infrastructure, emerging legislative and legal requirements, industry trends, best practices and increasing threats. Despite the perceived usefulness of EISA models, information architecture today still suffers from adoption problems. The critical influencing factors for adoption of enterprise information architectures models in Kenya have not been studied and understood. There is a need to increase adoption of enterprise information security architecture models in Kenya with special reference to Oil and Gas companies. This research intends to bridge that gap.

1.3 Justification of the study

Adoption and assimilation of information security architecture cannot be left to individuals, systems architects or individual departments. Having a cohesive approach for developing and maintaining a secure information security environment is a shared responsibility that goes beyond acquiring information security technologies and software. Information security architecture or practice brings to light the impact that information security can have on an organization's business processes as well as how it can improve security by following a framework for protection of valuable business assets, trade secrets, profitability and reputation. All of the best policies, standards, tools, methodologies and technologies mean nothing if an acceptable level of security is lacking. Information Technology keeps changing, and this underlines the need for an administrative approach in the implementation of information security.

It's no surprise that many an experienced security professional perceive the process of implementing information security in the same way as walking through a minefield. This perception hinders their initiatives in information security, thus compounding the risks. The need for a simplified approach to understanding the elements for adoption and assimilation of information security architecture is readily apparent. A common approach in implementing information security systems in organizations is to start by

writing policies and standards. However, this approach does not address business requirements for information security. This underlines the need to adopt an information security architecture framework.

1.4 Purpose of the Study

Enterprise Information Security Architecture is becoming a universal practice worldwide. The primary need for adopting enterprise information security architecture is to ensure that business strategy and IT security are aligned. Enterprise information security architecture allows traceability from the business strategy down to the underlying technology. The purpose of this study was to develop a simplified methodology for increased adoption and assimilation of information security architecture models in a complex environment with few security measures in place.

A Case Study was used to investigate information security architecture practices as an administrative innovation in selected Major Oil and Gas companies in Kenya using innovation diffusion theory and a model developed for Korean companies and to recommend a methodology in the Kenyan context to enhance adoption of information security architecture. The proposed methodology though based on the Oil and Gas Industry is built on robust adoption and assimilation models, and thus is capable of being used in other industries as well.

1.5 Objectives of the study

1.5.1 General Objective

Use a Case Study to investigate information security architecture practices as an administrative innovation in selected Major Oil and Gas companies in Kenya using a model developed for Korean companies and to recommend a methodology in the Kenyan context to enhance adoption of information security architecture. The proposed methodology though based on the Oil and Gas Industry is built on robust adoption and assimilation models, and thus is capable of being used in other industries as well.

1.5.2 Specific Objectives

i. To determine the impact of institutional influences in the adoption and assimilation of information security architecture as an administrative innovation;

ii. To ascertain the effects of institutional influences at different stages of adoption and assimilation;

iii. To examine the impact of moderating economic and organizational factors in the adoption and assimilation of information security architecture.

1.6 Research Questions

i. What is the impact of institutional influences in the adoption and assimilation of information security architecture as an administrative innovation?

ii. What are the effects of institutional influence at different stages of innovation adoption and assimilation,

iii. What is the impact of moderating economic and organizational factors on information security architecture adoption and assimilation?

1.7 Importance of the study

More and more companies are implementing different forms of enterprise security architecture to support the governance and management of IT. However, EISA models ideally relate more broadly to the practice of business optimization in that it addresses business security architecture, performance management and process security architecture as well. The slow adoption of EISA models presents several problems to the information security profession due to the disconnection between the business and the information security program. There is, arguably, a myopic view of security resulting from the fact information security practitioners are originally from the field of Information Technology. These practitioners literally "strayed" into the field of information security architecture and are largely unaware of the forces that drive the adoption game, which include organization, people and process. Thus the widely held view that information security architecture is a technological innovation

rather than an administrative innovation. Effective information security requires a balance among these elements.

By emphasizing a technical focus to information security architecture a gap is created between information security and the business units. Businesses are concerned with all types of risks including physical security, legal, financial and safety, in addition to information and technology. Too often, both sides fail to understand how all of these risks are interrelated (Anderson, 2008). The Information Security approach does not effectively address business requirements, and the expected costs outweigh the benefits. This is because the system and its configurations are not based on a comprehensive understanding and assessment of the enterprise's needs.

The information security systems are not based on business needs, are too generic and /or not tailored to meet the specific organization's needs. Effectiveness or reliability of the system largely depends on human ingenuity i.e. it is not process-driven. Cost of implementation does not compare favourably to benefits to be realized, if any, and this diminishes the value and reputation of security. There is also the restricted ability to embrace or satisfy business requirements, face competition, new products, for fear of risk.

What trends are occurring in the field? There is an increased need for adoption of information security architecture to match the inevitable surge in technology. Organizations are spending and hiring information security practitioners in record numbers, and legislation and regulations are proliferating. Despite all of these efforts, nearly every statistical measure of performance—from the number of incidents and vulnerabilities to the cost and impact of a breach—demonstrates that information security architecture is not yet in tandem with the organization's needs. Pouring more money and technology will not reverse this trend. In what other profession would a high level of investment be permitted with such poor return? (Anderson, 2008). Companies, therefore, need to embrace information security architecture as a key business enabler.

1.8 Scope of the Study

The study is concerned only with the adoption and assimilation of Enterprise Information Security Architecture (EISA) as an administrative innovation in large organizations in the Oil and Gas Industry in Kenya.

1.9 Definition of Terms

Operational Definitions:

Enterprise Information Security Architecture (EISA) is the process of instituting a complete information security solution to the architecture of an enterprise, ensuring the security of business information at every point in the architecture. In other words, it is the enterprise and its activities that are to be secured, and the security of computers and networks is only a means to this end.

Innovation is "any idea, practice, or material artifact perceived to be new by the unit of adoption" (Zaltman et al. 1973, p.158). **Administrative innovation** may be defined as the creation of a new organizational design that supports better the creation, production and delivery of products and services.

Diffusion may be defined as the spreading of ideas from one culture to another. **Diffusion of Innovations** may be defined as a theory of how, why, and at what rate new ideas and technology spread through cultures.

Assimilation may be defined as the incorporating of ideas into a culture and making them part of that culture, often taking on new characteristics.

Information Security Management as used in this study refers to the development of a security management program including the security policy, management committee, team structure (e.g. CISO or security officers), risk management process, and employee education to preserve the confidentiality integrity and availability of information in organizations.

Coercive Isomorphism refers to the political influence exerted by government agencies or powerful organizations such supervisory authorities within an industry. **Mimetic isomorphism** describes how organizations imitate other to be perceived as successful or legitimate. **Normative isomorphism** examines the collective influences resulting from the development of professionalization. (DiMaggio and Powell, 1991, Scott 1995).

CHAPTER TWO:
LITERATURE REVIEW

2.1 Introduction

There is a popular adage that "many a man on the road to success fails because he sets off from the wrong station". Before delving into adoption and assimilation of information security architecture, perhaps, it is worthwhile therefore to understand the goal of information security architecture? The goal (Gartner, 2006) is to "align security strategies between three functional areas of an organization. These are Business Architecture, Information Architecture (IA), and Technology Architecture, all three are explained in detail below. We introduce another two architectures, Security architecture and Enterprise Information Security Architecture, the latter being the main focus of our Study:

2.1.1 Business Architecture (BA)

Above all else, the security architecture must be aligned with the goals and objectives of the enterprise. Without proper alignment there will be an inevitable disconnect between business strategy and security. To enable this alignment it is vital to accurately outline the business architecture in place to achieve the objectives of the organization by asking several questions: What does the enterprise do? Who does it? What information do they use to achieve their goals? Where do they do it? By answering these questions it becomes possible for the security architecture framers to develop a comprehensive map of the strategies of the enterprise, along with a range of organizational charts and business process maps.

2.1.2 Information Architecture (IA)

Enterprises in today's complex world are experiencing rapid changes in constantly competitive situations. There is an increased need to be able to respond quickly to changing market conditions, new business opportunities, threats and emerging alliances that were unthinkable a few years ago (Wigand *et al.*, 1997, p. 1). Pressures

of global competition and growing dependence on information technology mean that the effective use of information is more important now than ever before. Enterprises have made substantial investments in information technology, but commitment to using information as a corporate resource appears to be lacking (Evernden and Evernden, 2003). The ease with which information can be created, extracted, and transmitted by e-mail and communication links has created expectations of the ability to exchange information faster and more frequently between enterprises and end-users.

Information is now recognized as a valid and valuable resource in the day-to-day management of an enterprise, the function described as information management has grown from being a pure library, filing or computing function to a mainstream management activity (Mahon and Gilchrist, 2004). From this evolutionary process the concept of "information architecture" has emerged in recent times. According to a number of sources the term "information architecture" was coined, or at least brought to wide attention, by Richard Saul Wurman in the mid-1970s at the American Institute of Architects' National Convention in Philadelphia with the conference theme entitled "Information Architects" (Evernden and Evernden, 2003).

Wurman's definition of an information architect according to Farnum (2002) and Wyllys (2001) is: an individual who organises the patterns inherent in data, making the complex clear; the person who creates the structure or map of information that allows others to find their personal paths to knowledge; and the emerging twenty-first century professional addressing the needs of the age focused on clarity, human understanding and the science of the organisation of information.

Morville (2004) and Farnum (2002) argue that although Wurnam's definition is helpful, its overall approach relates more to the visual design of information and emphasises Wurman's own background in designing printed media. Wurman's definition of information architecture can be construed as a way of abstracting from a complex situation or body of information and presenting those essentials in a clear

and aesthetically pleasing manner to the user (Wyllys, 2001). However, the notion of information architecture is not new. Brancheau and Wetherbe (1986) proposed the concept in 1986, using a high level map of the information requirements of an enterprise as an important aid to systems development. However, their model of IA excludes consideration of personnel and the organizational structures and challenges.

Information architecture is a foundation discipline describing the theory, principles, guidelines, standards, conventions and factors for managing information as a resource. It produces drawings, charts, plans, documents, designs, blueprints and templates helping everyone make efficient, effective, productive and innovative use of all types of information.

Using these plans, security architecture framers can understand the optimal flow of information within the enterprise. What applications are used to achieve the objectives of the business? What data do these applications require in order to achieve those objectives, and what integration methods are in place to enable the sharing of that information? Only by understanding these technologies and processes can it be possible for the framers to develop a strategy for ensuring the security of this data while allowing vital business processes to progress unimpeded.

2.1.3 Technology Architecture (TA)

Finally, it is necessary to study the technology architecture in place to support these applications and processes. The technology architecture of most enterprises is highly complex, involving a range of different technologies running on different platforms, each relying on a range of heterogeneous legacy systems. Ensuring the security of these technologies while allowing business processes sufficient access to information can be a daunting task. In order to ensure the security of data within this architecture it is necessary to build a map of every piece of that architecture, and to understand how information moves between its components.

2.1.4 Security Architecture (SA)

Security is applied by implementing industry standards and best practices such as ISO/IEC/27000, The Standard of Good Practices (SoGP) and Organization for Economic Cooperation and Development (OECP) Guidelines for the security of information systems. ISO/IEC and SoGP are considered to be the primary authority on standards".

2.1.5 Enterprise Information Security Architecture (EISA)

The field of Enterprise Information Security Architecture (EISA) has generated a lot of interest in the recent past. EISA was first presented by Gartner detailing how security should be incorporated into Enterprise Architecture. Most organizations lay claim to some form of information security architecture, however, documentation of the methodology for adoption of information security architecture is lacking. EISA can be viewed as the practice of applying a comprehensive and rigorous method for describing a current and/or future structure and behavior for an organization's security processes, information security systems, personnel and organizational sub-units, so that they align with the organization's core goals and strategic direction. Although often associated strictly with information security technology, it relates more broadly to the security practice of business optimization in that it addresses business security architecture, performance management and security process architecture as well. EISA is not a process for building a wall to shield the information systems of an enterprise but is the architecture that ensures information security aligns with the strategies and objectives of the enterprise while promoting seamless integration.

Architecture has its origins in the building of magnificent houses in cities and towns and this sense is well understood by everyone. Architecture, in the traditional context, is a set of rules and conventions by which buildings are created which serve the intended purpose, both functionally and aesthetically. The concept of architecture is "one that supports our needs to live, to work, to do business, to travel, to socialize and to pursue our leisure. In the context of designing and building business computer systems, the term has been adopted to mean "the rules and standards for the design

and construction of computers, communication networks and the distributed business systems that are implemented using these technologies" (Sherwood, Clark and Lynas, 2005).

In line with the above background, clearly information security architecture goes beyond the technology that an organization adopts for its business. The goal of Information security architecture is to help the enterprise achieve objectives in the current operational constraints or environment. This broader view of information systems architecture underlines the fact that technological factors are not the only drivers influencing the architecture. Rather it is only one of the considerations. Organizations that have overlooked this fact often end up with architectures that fail to meet their business needs.

The greatest challenge in information security is aligning with business objectives. A 2007 survey by Deloitte and Touche LLP and Panemon Institute showed that 50 percent of North American security professionals' time is spent on reactive and tactical activities such as remediation of operational vulnerabilities. This disconnect between information security operations and strategic business objectives adds pressure to increased security spending while risks, incidents and losses continue to escalate. A framework that enables information security professionals to align their activities with their organization's business is needed (Anderson, 2008).

Business enterprises in developing economies perceive information security as a "nice-to-have". Most of the large financial sector-based enterprises, which are more risk-conscious, implement information security as a gimmick to attract customers. It helps project a good image to customers. Others implement information security systems to comply with requirements mandated by parent companies, or dictated by regulatory requirements. Generally the lower the potential to cause financial loss, the less attention accorded to information security requirements. There are those who have the perception that information security is not an immediate threat.

Generally, even where a company has the means to address information security, the implementation approach is deficient and cannot meet business requirements. The agility required to respond to the ever-present technological threats is lacking. The reason for this, according to a white paper published by Sherwood, Clark, Lynas (2005), is that "usually a requirement is identified and a solution sought and acquired to meet that requirement without regard to the broader implications. A tactical solution is implemented which is often effective in providing some security, but frequently no-one is really sure that the security is appropriate to the risk, or that the cost is commensurate with the benefit, or that it meets a wide variety of other business requirements which are not specifically risk-related. Security is often the last thing to be considered in business information design, and often gets relegated to the status of a few add-on fixes when all other design decisions have been frozen."

Sherwood, Clark, and Lynas captured the potential problems of the above approach in their white paper by stating that "the security solutions are often isolated and incapable of being integrated together or of inter-operating with one another. The variety of security solutions leads to increased complexity and cost of support, and in particular can lead to an exploding workload with regard to administration and management. Worst of all, because there has been inadequate attention paid to the business requirements, the "solution" can sometimes hinder the business process rather than helping it, and the reputation of "security" among the business community gets worse and worse."

2.2 Theoretical Background

Current literature clearly shows that researchers have been using diverse approaches and theoretical frameworks in conducting research in the field of information security. However, other than Hsu et all (2009) who argued for it as "a legitimate and well-suited theoretical lens", research so far has not been done on adoption and assimilation of information security as an administrative innovation. Furthermore, none has studied information security (architecture) as an innovation in general, or an administrative innovation in particular.

2.2.1 Information Security Architecture as an Administrative Innovation

Researchers have used different theoretical lenses to critically assess information security research. Dhillon and Backhouse (2001) applied Burrell and Morgan's framework, whereas Siponen (2005) analyzed five classes of traditional information security methods. Recently, Siponen and Willison (2007) examined information security research between 1999 and 2004 via Laudan's reticulated model of science. Whereas each of these models advances our understanding of information security, none view the phenomenon as an innovation in general, or an administrative innovation in particular, which, we argue, is a legitimate and well-suited theoretical lens.

The theoretical lens applied in the current study is one that views information security is an administrative innovation rather than a technological innovation. Technological innovation would focus on developments in security technologies, whereas Information Security Architecture fits with the philosophy of administrative innovation because, as defined in this study, it refers to the development of a Security Architecture program including the security policy, management committee, team structure e.g., CISO or security officers, risk-management process, and employee education to preserve the confidentiality, integrity, and availability of information in organizations. The implementation of such a program involves restructuring and investment in human resources and knowledge development through different levels of organization. This is similar to what Teece (1980, p. 465) describes as the requirement of "major reassignment of tasks and responsibilities."

When security is treated as a technological innovation, research is normally placed under the umbrella of "computer security." This perspective has been the dominant research perspective for the past few decades (Siponen and Willison 2007, Straub et al. 2008). Viewing information security as a technological innovation and with an eye to investment, Cavusoglu et al. (2004, 2005) studied the value of IT security architectures, while Gordon and his colleagues researched the economics of the information security capital expenditures (Gordon and Loeb, 2001, 2002). However

useful this perspective is, some scholars have argued that research based on the technological innovation paradigm has significant limitations. Dhillon and Backhouse (2001, p. 145) explain that these technical-centric approaches are not appropriate or sufficient "when organizational structures become flatter and more organism-like [sic] in their nature."

Echoing these perspectives, in recent years, Ransbotham and Mitra (2009, p. 122) say that "research on the organizational perspective (of information security management) is limited but emerging." Such studies appropriately characterize what we see as administrative innovations in information security management. This very different stress on the essentially managerial nature of information security is relevant for a number of reasons. As Straub et al. (2008, p. 5) observe, it likewise indicates as clearly as possible that the likely problem today is not the lack of technology, but its intelligent application. The management of Information Security Architecture is in its infancy.

This viewpoint was supported by our observation that although many organizations have adopted information security practices during the last decade (Backhouse et al. 2006, Hsu 2009, Ransbotham and Mitra 2009), it is still difficult to make the business case to top management that increased investment in information security is necessary as a successful information security program. If information security should be studied as an administrative innovation, how shall we go about this? First, administrative innovation requires precise interpretation of definitions and enumeration of procedures even though "variation in the form of adoption may be especially high" (Westphal et al. 1997, p. 367). Damanpour (1991, p. 561) argues that administrative innovations are "more directly related to its management," while Ransbotham and Mitra (2009, p. 122) indicate that Information Security Architecture focuses on "managerial actions that promote a secure environment." Goodhué and Straub (1991) argue that managers' concerns over systems security risk differ because of their individual characteristics and their interpretation of the surrounding organizational environment.

Thus, because of the managerial orientation of the implementation process, there are likely to be variations in the way it is managed. In other words, decision makers may interpret Information Security Architecture requirements in different ways, and this will impact the scope and scale of adoption and assimilation. Second, in that information security implementation is typically much larger than a one-off project, the adoption of Information Security Architecture involves continuous security architecture improvement and change management to adapt to varying environmental contingencies. This philosophy fits the notion of an administrative innovation that emphasizes the issue of organization-environment co-alignment (Venkatraman et al. 1994). Straub and Welke (1998) argue that, with formalized security planning and ongoing feedback within the organizational structure, managers become more aware of security problems, and this allows them to find appropriate solutions more easily.

Third, the diffusion of administrative innovations is associated with ongoing changes in an organization's social structure. In information security management, the notion of employee awareness and security culture is an important element of policy. Management initiatives in the form of security training programs and rewards for security-related behavior can lead to the creation of a security culture (Ramachandran and Rao 2006). That is, the success of Information Security Architecture management depends on the extent to which employees comply with the policy and demonstrate a high level of security awareness and knowledge. Therefore, information security managers should continually expand employees' knowledge so they can "deal with exceptional situations in which information security policies are in conflict with the business objectives of organizations" (Siponen and Iivari 2006, p. 468). This implies that, to assimilate Information Security Architecture and cultivate a security culture, organizations must be able to induce changes in employee attitudes as well as their sense of responsibility toward information security.

2.2.2 Institutional Pressure for Information Security Architecture Adoption

Based on these arguments on administrative innovations and, in particular, information security innovations, it needs to be noted that, according to neo-institutional theorists, practices travel from one organization to another as a result of social isomorphism (Scott 1995). Researchers on isomorphism describe three mechanisms that make up these institutional forces, namely, coercive, mimetic, and normative isomorphism (Dimaggio and Powell 1991, Scott 1995). First, coercive isomorphism refers to the political influence exerted by government agencies or powerful organizations such as supervisory authorities within an industry. Second, mimetic isomorphism describes how organizations imitate other organizations to be perceived as successful or legitimate. Institutional mimicry is more likely to occur for competitive reasons or as a strategy to address uncertainties and ambiguities (Guler et al. 2002, Tingling and Parent 2002). When organizations are able to access the same information about emerging security risks and best practices, they engage in a "learning mimicry" (Guler et al. 2002, p. 216) by adopting similar risk-management strategies.

According to Hsu (2009), this competitive mimicry has influenced the institutionalization process of information security certification in the Taiwan financial industry. Third, normative isomorphism examines the collective influences resulting from the development of professionalization. DiMaggio and Powell (1991, p. 71) observe that the "mechanism for encouraging normative isomorphism is the filtering of personnel," while Hu et al. (2006, 2007) note that "the impact of normative forces seem to be more selective and context specific" (Hu et al. 2006, p. 7) and thus varies among individuals in an organization. The context dependent nature of normative pressure is also evident in the work of Teo et al. (2003).

2.3 Technology Adoption Frameworks

The adoption of new technologies has been studied through different theoretical frameworks, which include the Diffusion of Innovation Theory; Rogers (1995), the Theory of Reasoned Action; Fishbein and Ajzen, (1975), theory of planned behaviour; Davis, (1989) among others.

2.3.1 Technology Acceptance Model

Technology Acceptance Model (TAM) has been widely used by information technology (IT) researchers to gain a better understanding of IT adoption and its use in organisations. It has been used in very different settings, e.g. to test the acceptance of: computer technology (Davis *et al.*, 1989), online shopping (Gefen *et al.*, 2000a), mobile computing (Wu *et al.*, 2007), e-commerce (Pavlou, 2003), and e-Government services (Carter and Bélanger, 2005).

The theoretical foundation for TAM is based on Fishbein and Ajzen's theory of reasoned action (TRA) (Fishbein and Ajzen, 1975). Davis *et al.*, (1989), the TAM proposed that two particular beliefs are the main drivers for technology acceptance: perceived usefulness ("the degree to which a person believes that using a particular system would enhance his or her job performance") and perceived ease of use ("the degree to which a person believes that using a particular system would be free of physical and mental efforts). Perceived usefulness and perceived ease of use influences one's attitude towards system usage, which influences one's behavioural intention to use a system, which, in turn, determines actual system usage (Davis *et al.*, 1989). However, the external variables that impact the perceived usefulness and perceived ease of use are not completely explored in the TAM. Davis *et al.* (1989) also found that attitude did not fully mediate perceived usefulness and perceived ease of use. Based on these findings, therefore, a more parsimonious TAM was suggested which removed the attitude towards usage construct from the model (Carter and Bélanger, 2005).

2.3.2 Extended Technology Acceptance Model

Venkatesh and Davis (2000) proposed an extension of TAM (TAM2) by adding more important determinants of perceived usefulness – that is, subjective norm, image, job relevant, output quality, result demonstrability, and perceived ease of use – and two moderators – that is, experience and voluntariness (Venkatesh and Davis, 2000). In addition to this, in the TAM2, it omits attitude toward using because of weak

predictors of either behavioral intention to use or actual system usage (Venkatesh and Davis, 2000; Wu *et al.*, 2007).

Venkatesh and Davis, (2000), TAM2 consists of social influence and cognitive instrumental processes as the determinants of perceived usefulness. The social determinants are subjective norm ("the degree to which an individual perceives that most people who are important to him think he should or should not use the system"), and image ("the degree to which an individual perceives that use of an innovation will enhance his or her status in his or her social system"). The cognitive determinants are: job relevance ("the degree to which an individual believes that the target system is applicable to his or her job"), output quality ("the degree to which an individual believes that the system performs his or her job tasks well"), and result demonstrability ("the degree to which an individual believes that the results of using a system are tangible, observable, and communicable") (Venkatesh and Davis, 2000; Venkatesh and Bola, 2008). Experience and voluntariness were included as moderating factors of subjective norm (Venkatesh and Davis, 2000).

2.3.3 Theory of Reasoned Action

The Theory of Reasoned Action (TRA) was proposed by Fishbein and Ajzen (1975) to explain and predict the people's behavior in a specific situation. TRA is a well-known model in the social psychology domain. According to TRA a person's actual behavior is driven by the intention to perform the behavior. Individual's attitude toward the behavior and subjective norms are the 'loading factors' toward behavioral intention. Attitude is a person's positive or negative feeling, and tendency towards an idea, behavior. Subjective norm is defined as an individual's perception of whether people important to the individual think the behavior should be performed.

The Theory of reasoned action is a more general theory, and has been applied to explain behavior beyond the adoption of technology. However, when applied to adoption behavior, the model includes four general concepts - behavioral attitudes, subjective norms, intention to use and actual use. The inclusion of subjective norm

represents an important addition. In TRA, subjective norm is composed of the user's perception of how others think she should behave, and her motivation to comply with the expectations of these referents, Fishbein and Ajzen, (1975). TRA has been applied in its original form to explain the adoption of ICT-applications, Liker and Sindi (1997), but typically TRA is used as a basis for modifying the TAM-model with subjective norm as suggested above, Venkatesh and Morris, (2000).

2.3.4 Theory of Planned Behaviour

The theory of planned behavior was proposed as an extension of the theory of reasoned action to account for conditions where individuals do not have complete control over their behaviour Ajzen (1985). However, this theory also included determinants of the behavioral attitude and subjective norm. Models based upon TPB have been applied to the explanation of different types of behavior, but when applied to the adoption of ICT systems or services, the model contains five concepts - behavioral attitudes, subjective norm, behavioral control, intention to use and actual use. The components of behavioral attitude and subjective norm are the same in TPB as in TRA. In addition, the model includes behavioral control as a perceived construct. Perceived behavioral control reflects the internal and external constraints on behavior, and is directly related to both intention to use and actual use. Consequently, actual use is a weighted function of intention to use and perceived behavioral control. TPB has been applied to explain the adoption of such diverse systems as spreadsheets Mathieson (1991), computer resource centers Taylor $Todd (1995), and recently, electronic commerce services Battacherjee (2000). The role of subjective norm in TPB when compared to TAM is however somewhat unclear.

2.3.5 Diffusion of Innovation Theory

The Diffusion of Innovation theory (DOI) is another model also grounded in social psychology. Since 1940's the social scientists coined the terms diffusion and diffusion theory (Rogers, 1983). This theory provides a framework with which we can make predictions for the time period that is necessary for a technology to be accepted. Constructs are the characteristics of the new technology, the communication networks and the

characteristics of the adopters. We can see innovation diffusion as a set of four basic elements: the innovation, the time, the communication process and the social system. Here, the concept of a new idea is passed from one member of a social system to another. Moore and Benbasat (1991) redefined a number of constructs for use to examine individual technology acceptance such as relative advantage, ease of use, image, compatibility and results demonstrability.

2.3.6 Significance of DOI and TAM

On a more general level the adoption of information technology has been widely researched in the economics and information systems domains. Theories such as the diffusion of innovations theory and the technology acceptance model have been applied to explain the adoption and diffusion of a great variety of innovations ranging from new methods of agriculture to modern communication technology. (Rodgers 2006). However, there are no recorded studies that use these theories to examine the adoption and assimilation of Information Security Architecture as an administrative innovation.

As our Study focuses on the adoption and assimilation of Information Security Architecture as an administrative innovation, the above theories have been selected: TAM has been used for studying factors that might motivate organizations to invest (or not to invest) in information security, hence suited to adoption. TAM proposes that perceived usefulness and ease of use of information security influence investment decisions. TAM further proposes that seven other variables influence perceived usefulness and ease of use. They are: external environment, prior information security experiences, perceived risks of not securing information, information security budget, security planning, confidence in information security, and security awareness and training. DOI is suited to assimilation of information security architecture.

2.4 Theoretical Framing

From an institutional perspective, firms face pressures to conform from regulatory bodies or other peer organizations. Nevertheless, there is also evidence that firms can

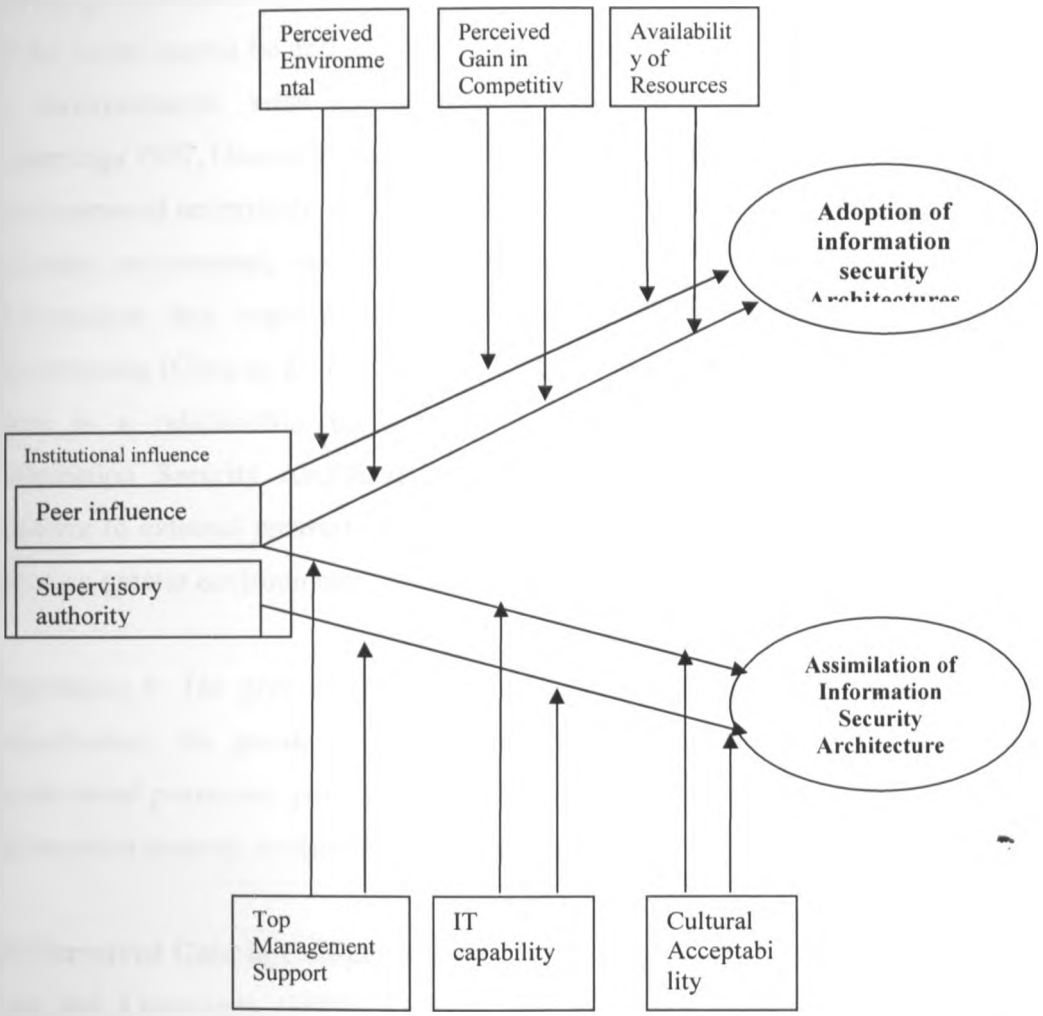
formulate different strategic decisions in response to external legitimacy pressures (Ang and Cummings 1997, Oliver 1991, Perrow 1985). In addition to institutional pressure on adoption, a number of studies also point out the relevance of environmental factors in the post-adoption context (Hirt and Swanson 2001, Gosain 2004). For instance, Butler (2003, p. 215) elaborates on the "institutional tension" among various social actors during the development of Web-based IS development due to their commitments to the external "communities of practices we argue that, while acknowledging institutional effects, firms might exhibit different attitudes towards information security Architecture adoption and assimilation because of the influence of various internal and external organizational contingencies. In other words, given the institutional pressure to conform, these contingencies affect the extent to which organizations attribute importance to information security Architecture as an administrative innovation.

2.5 Proposed Enhanced Research Model for Adoption of Information Security Architecture

In conducting our Study, we have taken the approach developed by Hsu et al (2009) in that their extensive research on Korean companies titled "Institutional Influences on Information Systems Security Innovations" investigated information security management as an administrative innovation. Due to the similarities in the research objectives, we have adopted their research model. The result of their two-step method was an enhanced research model of Information Security Architecture adoption, as shown in Figure 1 below. Drawing from the institutional theory on innovation diffusion, organizational decision to adopt and assimilate Information Security Architecture is influenced by the supervisory authority and peer organizations. As mentioned earlier, administrative innovation can lead to different forms of adoption. Given the nature of administrative innovation, which is a management-oriented and continuous phenomenon, we expect that moderating variables will differ between the adoption and assimilation stages. In Information Security Architecture, adoption can range from a simple security policy, standardizing on the ISO/IEC 27002 framework, for instance, to an enterprise-wide security architecture implementation. Each

scenario involves different levels of investment. In contrast to adoption decisions, our argument is that the assimilation of an administrative innovation is normally coupled with the process of organizational change; that is, success will depend on the organization's ability to manage the assimilation process.

Figure 1: Research Model for adoption of EISA



Source: Hsu, Lee, and Straub: Institutional Influence on IS Security Innovations.

Description of The Research Model

2.5.1 Economic-Based Adoption factors

(a) Perceived Environmental Uncertainty

Organizational theorists have long been interested in the relationship between organizations and their environments and argued that coping with uncertainty is a vital organizational survival skill (Duncan 1972, Milliken 1987). Pfeffer and Salancik (1978, p. 67) define environmental uncertainty as "the degree to which future states of the world cannot be anticipated and accurately predicted." One strategic response to environmental volatility involves interorganizational imitation (Ang and Cummings 1997, Haunschild and Minner 1997). In information security management, environmental uncertainty refers to the unpredictability of major trends or risks in the business environment, and the possible security risks induced by the emerging technologies that organizations deploy to enhance operational efficiency and effectiveness (Chou et al. 1999, Straub et al. 2008). Chang and Ho (2006) show that there is a relationship between environmental uncertainty and implementing Information Security Architecture. Therefore, we hypothesize that organizations conform to external pressures to adopt information security Architecture when they perceive greater environmental uncertainty.

Hypothesis 1: *The greater the level of environmental uncertainty perceived by an organization, the greater the likelihood that the organization will conform to institutional pressures; peer influence and supervisory authority influence to adopt information security Architecture innovations.*

(b) Perceived Gain in Competitive Advantage

Ang and Cummings (1997) observed that firms are more likely to conform to institutional requirements if doing so results in a gain in production economics. In the hypercompetitive and globalized business environment, organizations and market participants increasingly find it necessary to deploy signaling strategies to potential customers and business partners that differentiate their products and services from

those of lower quality. Kankanhalli et al. (2003) also argue that management investment in effective Information Security Architecture can lead to competitive advantages. Therefore, we hypothesize that when an organization perceives an increase in its competitive advantage, it is expected to conform more completely to institutional influences on Information Security Architecture adoption.

Hypothesis 2: *The greater the gain in competitive advantage perceived by an organization, the greater the likelihood that the organization will conform to institutional pressures peer influence and supervisory authority influence to adopt information security Architecture innovations.*

(c) Availability of Resources

Discussing the economic determinants of organizational innovation, Rosner (1968) contended that the resources available to an organization determine whether it can afford innovation. Other researchers have shown the moderating effect of available resources in response to institutional pressure (Ang and Cummings 1997, Zinn et al. 1998). Available resources allow firms to be flexible in investing in additional human resources for administrative innovation as well as in absorbing failure costs (Kaluzny et al. 1993), which is important when organizations have difficulty achieving a return on investments. In terms of information security, Straub et al. (2008,) explain that Information Security Architecture is also an "economic decision" and it usually "requires resources." Firms with larger resources, ones that can tolerate more risk and engage in larger investments in security management, hence are more likely to conform to institutional pressure.

Hypothesis 3: *The greater the availability of organizational resources, the greater the likelihood that the organization will conform to institutional pressures peer influence and supervisory authority influence to adopt information security Architecture innovations.*

2.5.2 Organizational Capability-Based Assimilation Factors

(a) Top Management Support

Damanpour (1991) argues that managerial support is "especially required in the implementation stage, when coordination and conflict resolution among individuals and units are essential" (p. 558). Bantel and Jackson (1989) discuss the significance of the top management team in relation to innovation decision-making in the banking sector. In addition, it has been found that the role of top management is much more important in the assimilation stage than in the adoption process (Liang et al. 2007). Thus, the strong participation of top management results in the implementation of an efficient innovation process and activities intended to assimilate these innovations in the organization (Ba et al. 2001). Information Security Architecture literature point to the importance of top management in supporting information security Architecture programs in organizations. Thus, we hypothesize that stronger top management support will lead to a higher degree of adoption of Information Security Architecture innovations.

Hypothesis 4: *The greater the top management support, the stronger the relationship between institutional influences peer influence and supervisory authority influence and information security Architecture adoption.*

(b) IT Capability

Bharadwaj (2000, p. 171) defines IT capability as "an ability to mobilize and deploy IT-based resources in combination or copresent with other resources." The capability allows an organization to connect people to people as well as people to innovation activities, such as information security Architecture (Junarkar 1997). We argue that IT capability is especially important when the nature of the innovation is administratively oriented. With a sufficient IT infrastructure, firms can quickly adjust to changing environmental contingencies and facilitate the organizational learning process. Chang and Ho (2006) also found a positive relationship between business managers' IT competence and the implementation of information security

management. Furthermore, while the importance of the information security maturity model has been emphasized in prior literature, a recent interesting view is that the degree of information security maturity needs to be assessed using a capability perspective (Chiang et al. 2008). Aligning with that perspective, our qualitative interviews with practitioners also highlighted the importance of the IT capability. Many interviewees emphasized IT capability as a key factor of Information Security Architecture adoption. Based on the above discussion, we hypothesize that when IT capability is high firms are more inclined to conform to external pressures to assimilate Information Security Architecture.

Hypothesis 5: *The greater an organization's IT capability, the stronger the relationship between institutional influences peer influence and supervisory authority influence and information security Architecture adoption.*

(c) Cultural Acceptability

Similar to the line of argument on IT capability articulated above, cultural acceptability plays an equally vital role in supporting the creation of a security culture and the enhancement of employees' security awareness during the adoption stage. In framing an information security strategy, Baskerville and Dhillon (2008) identify several competencies required to manage information security, e.g. the competence to maintain policy flexibility, the competence to communicate the necessity for information security procedures, and the competence to facilitate informal communication about Information Security Architecture. In her empirical investigation on IS security certification implementation in a financial institution, Hsu (2009) found that the lack of organizational culture partly contributes to the ineffectiveness of IS security Architecture implementation because employees did not change their attitude and behaviors about IS security.

Hypothesis 6: *The higher the cultural acceptability of innovation, the stronger the relationship between institutional influences peer influence and supervisory authority influence and information security Architecture adoption.*

CHAPTER THREE
RESEARCH METHODOLOGY

3.1 Research Design

The research design that was employed in this study was a descriptive research design in form of a survey. This was augmented with qualitative techniques such as interviews. Hence, overall, the study adopted a mixed methods approach. The hypothesized research model was tested empirically via a questionnaire that collected data about information security architecture projects in five major oil companies in Kenya. Data was gathered from each organization one at a time over a period of three months. In keeping with the desire to capture information security architecture practices as administrative innovations, the unit of analysis was organizations that were either in the process of implementing or had already begun implementing enterprise-wide information security initiatives. The major purpose of descriptive research design was to describe the state of affairs as it is at present. According to Mugenda and Mugenda (1999) a descriptive research is a process of collecting data in order to answer questions concerning the current status of the subjects in the study. These descriptions of a descriptive research matches with the purpose of this study.

3.2 Target Population

According to Ngechu (2004), a population is a well-defined set of people, services, elements, events, group of things or households that are being investigated. This definition ensures that population of interest is homogeneous. And by population the researcher means complete census of the sampling frames. Population studies also called census are more representative because everyone has an equal chance to be included in the final sample that is drawn according to Mugenda and Mugenda (1999). The population of interest for this study were companies in the oil and gas industry in Kenya. Currently there are 17 major Oil and Gas companies in Kenya out of which we targeted 5 of them (+1 State Owned National Oil Company of Kenya) for our Study being the major players in the industry with a capacity to embrace information security architecture.

3.3 Sampling and Sample Size

Purposive sampling was used to select large institutions in the Oil and Gas industry in Kenya. The criterion used in the selection of these companies was their published market share as shown in Appendix III. The sample size for the study was therefore 5 large institutions in the Oil and Gas industry, with a preliminary in depth study being done in Gulf energy. The sample from the population was selected on the basis of suitability for the objective research, as a matter of convenience. The Study being a survey meant that questionnaires were distributed to all selected Oil and Gas companies in Kenya; senior management level employees were selected from the IT departments of each of the five large institutions in the Oil and Gas industry.

3.4 Data Collection

In order to identify the information security architecture of large institutions in the Oil and Gas industry, self-administered drop and pick questionnaires were distributed among sampled employees currently employed by 5 large institutions in the Oil and Gas industry. Questionnaires were designed in line with the research objectives. The questionnaires were developed to test the proposed hypothesis. The questionnaires had open ended questions, close-ended questions and Likert questions. The close-ended and lirket questions provided more structured responses to facilitate tangible recommendations. The open-ended questions provided additional information that may not have been captured in the close-ended and Likert questions. Secondary data sources were employed through the use of previous documents or materials to supplement the data that was received from questionnaires.

3.5 Reliability and Validity of the Instrument

3.5.1 Pilot Test Report

A pilot study was first carried out in Gulf Energy, one of the companies in the Oil and Gas industry in Kenya, which was not be included in the actual survey. The pilot study enabled the researcher to be familiar with research and its administration procedure as well as identify items that required modification. The results helped the

researcher to correct inconsistencies arising from the instruments, which ensured that they measured what was intended. Reliability refers to the consistency of measurement and is frequently assessed using the test–retest reliability method. Reliability is increased by including many similar items on a measure, by testing a diverse sample of individuals and by using uniform testing procedures. Reliability of the research instrument was enhanced through the pilot study which allowed for pre-testing of the research instrument. The clarity of the instrument items to the respondents was established so as to enhance the instrument's reliability.

3.5.2 Reliability Analysis

Reliability of the questionnaires was evaluated through Cronbach's Alpha which measures their internal consistency. The Alpha measures internal consistency by establishing if a certain item measures the same construct. Nunnally (1978) established the Alpha value threshold at 0.6 which the study benchmarked against. Cronbach Alpha was established for every objective in order to determine if each scale (objective) would produce consistent results should the research be done later on. Table 4.1 below shows that perceived environmental uncertainty had the highest reliability (α=0.885) followed by perceived gain in competitive advantage components (α=0.769), then IT Capability (α = 0.735) then cultural acceptability (α=0.731), Availability of Resources (α = 0.633) and top management support (α=0.601). The overall value of Cronbach Alpha was valued at 0.725. This illustrates that all the four scales were reliable as their reliability values exceeded the prescribed threshold of 0.6, thus the instrument was reliable to use in collecting data and this helps to achieve the desired research objective.

Table 1: Reliability Coefficients

Scale	Cronbach's Alpha	Number of Items
Perceived Environmental Uncertainty	0.885	5
Perceived Gain in Competitive Advantage	0.769	5
Availability of Resources	0.633	4
Top Management Support	0.601	5
IT Capability	0.735	6
Cultural Acceptability	0.731	3
Overall	0.725	

3.6 Data Analysis

Before analyzing the data completed questionnaires were edited for completeness and consistency. A content analysis and descriptive analysis was employed. The content analysis was used to analyze the respondents' views about information security architecture. The data was coded to enable the responses to be grouped into various categories. Descriptive statistics, such as frequency, percent and weighted means, were used to help in data analysis. Tables were used to present the data collected for ease of understanding and analysis. Appropriate designed scales were used to measure the two independent variables (i.e. institutional influence, which included both peer influence and supervisory authority influence) two dependent variables (i.e. adoption and assimilation of information security innovations), and six moderating variables. Multiple five-point Likert scales from "strongly agree" to "strongly disagree" were used to assess each of the variables.

Measures were based not only on previously validated instruments but also on conceptual definitions and theoretical statements drawn from the literature. For example, the institutional influences of information security architecture, such as social pressure to conform, arise primarily from peer organizations and supervisory authorities (Ang and Cummings 1997).

To account for extraneous sources of variation in the adoption and assimilation stages, we added control variables for organization size, IT budget, industry type, information security architecture adopted, and the length of time after the most recent information security practice was adopted. Organizational capability was measured in terms of total market share, while the IT budget was assessed as a percentage of total revenues.

CHAPTER FOUR:
DATA PRESENTATION, ANALYSIS AND INTERPRETATION

4.1 Analysis Method

Descriptive statistics were used to analyze the data. In the descriptive statistics, relative frequencies were used in some questions and others were analyzed using mean scores with the help of Likert scale ratings in the analysis.

Factor Analysis was used to analyze large numbers of dependent variables to detect certain aspects of the independent variables affecting those dependent variables - without directly analyzing the independent variables. It enabled us to reduce the number of elements to be studied and to observe how they are interlinked.

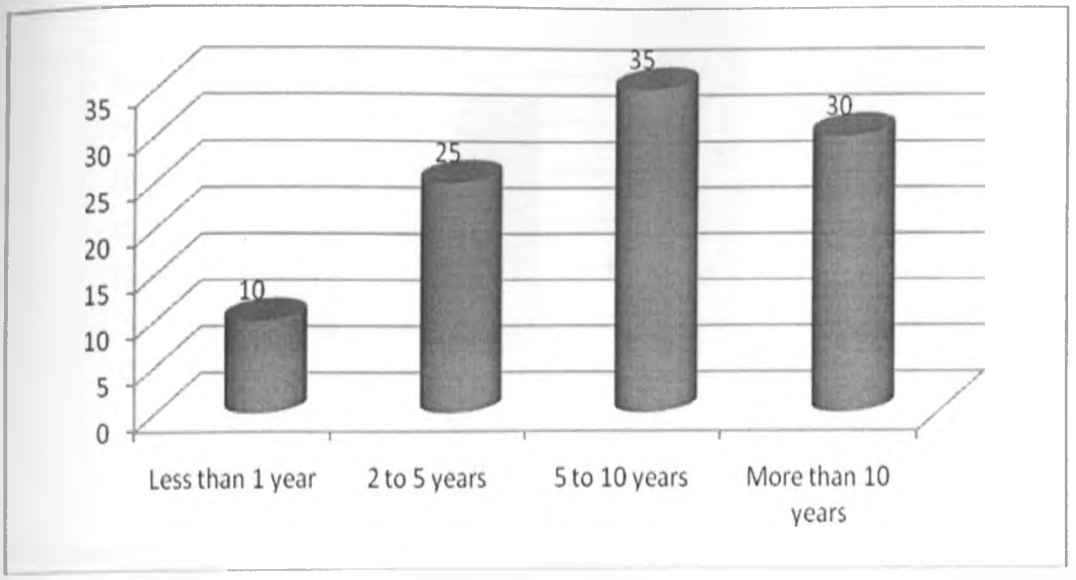
Regression Coefficients were used to interpret results by identifying where the t-test for a regression coefficient was not statistically significant, and avoid reaching incorrect conclusions on dependence among the variables.

Correlation was used to measure the relationship between variables. Possible correlations range from +1 to –1. A zero correlation indicates that there is no relationship between the variables. A correlation of –1 indicates a perfect negative correlation, meaning that as one variable goes up, the other goes down. A correlation of +1 indicates a perfect positive correlation, meaning that both variables move in the same direction together.

4.2 Statistical Analysis of Respondents

The respondents were from the 5 major oil and gas companies in Kenya which at the time of this Study are (1) KenolKobil, (2) Kenya Shell, (4) Total Oil (Kenya) Limited, (5) Oil Libya, and (6) National Oil Company of Kenya (NOCK). Their market share as provided by the Energy Regulatory Board (Appendix III) is a clear indication of the size of the companies.

Figure 2: Length of time in the company



Source, Author (2012)

From the findings on the length of time the respondents had been in their respective companies, the study found that most of the respondents as shown by 35% indicated that they had worked in their respective companies for 5 to 10 years, 30% of the respondents indicated that they had been in their respective companies for more than 10 years, 25% of the respondents indicated that they had been in their respective companies for 2 to 5 years whereas 10% of the respondents indicated that they had been in the company for less than 1 year.

Figure 3: Distribution of respondents by gender

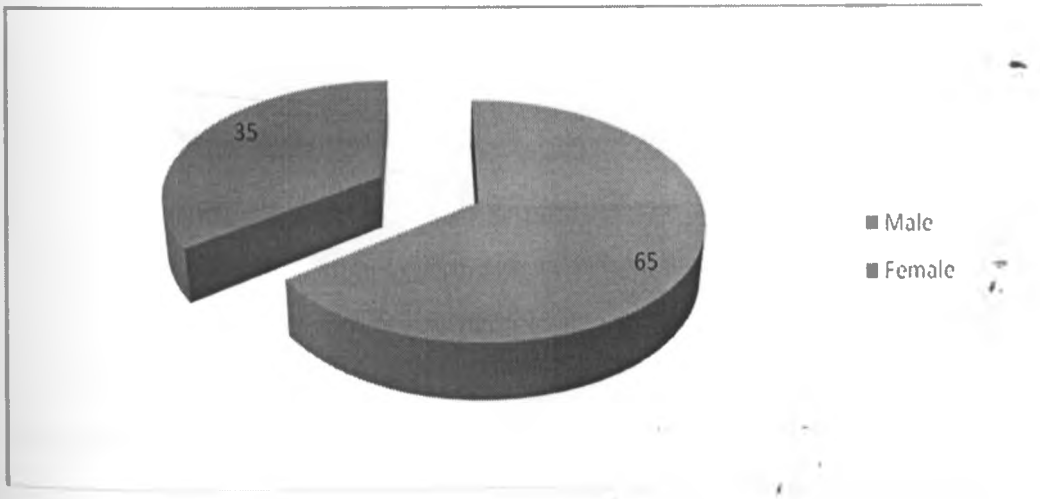
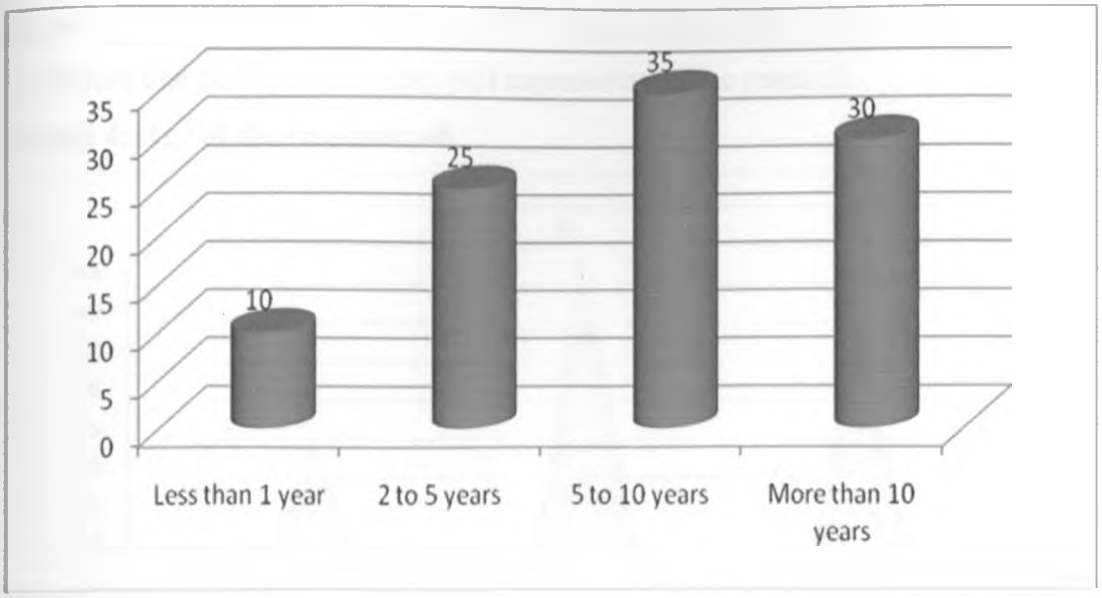


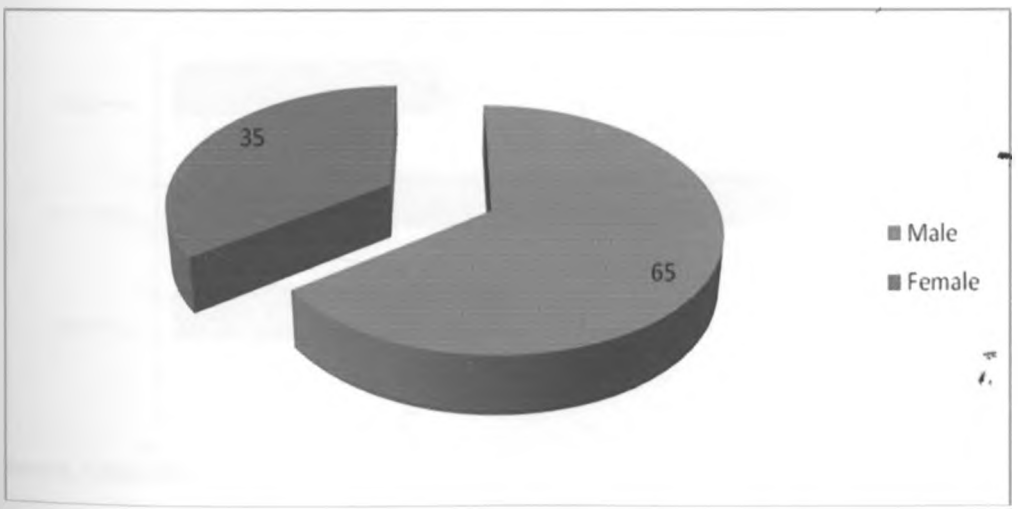
Figure 2: Length of time in the company



Source, Author (2012)

From the findings on the length of time the respondents had been in their respective companies, the study found that most of the respondents as shown by 35% indicated that they had worked in their respective companies for 5 to 10 years, 30% of the respondents indicated that they had been in their respective companies for more than 10 years, 25% of the respondents indicated that they had been in their respective companies for 2 to 5 years whereas 10% of the respondents indicated that they had been in the company for less than 1 year.

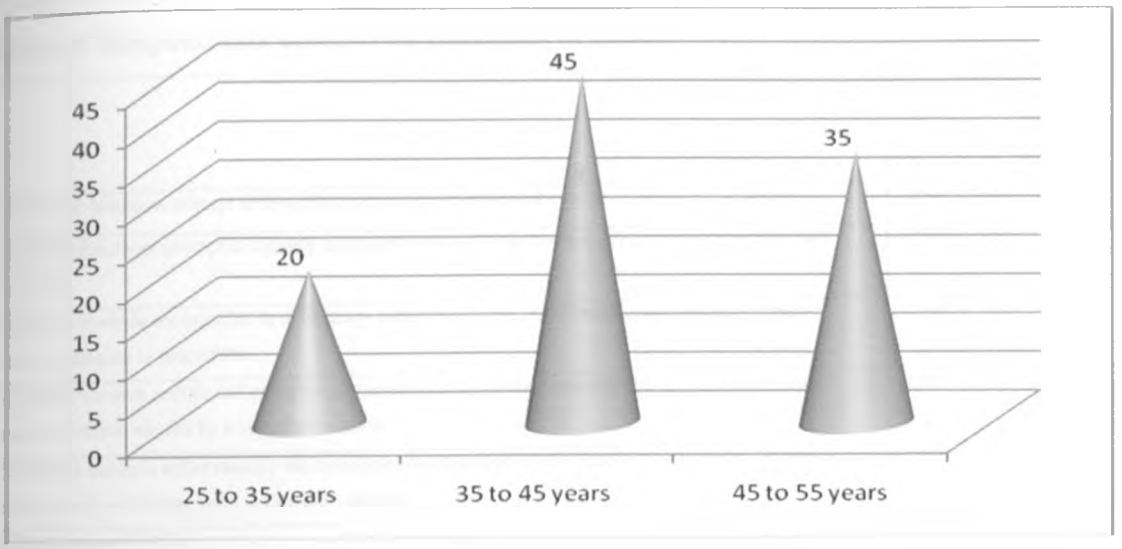
Figure 3: Distribution of respondents by gender



Source, Author (2012)

On the gender of the respondents, the study found that majority of the respondents as shown by 65% were male whereas 35% of the respondents were female. This is an indication that both genders were well represented in the research.

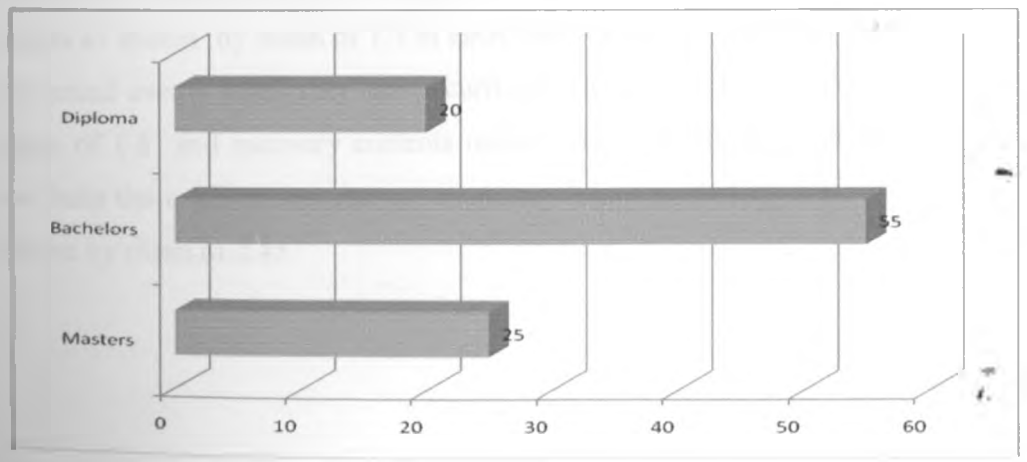
Figure 4: Age of the respondents



Source, Author (2012)

From the findings on the age of the respondents, the study found that most of the respondents indicated 35 to 45 years, 35% of the respondents indicated 45 to 55 years whereas 20% of the respondents indicated 25 to 35 years. This shows that respondents were well distributed in terms of their age.

Figure 5: Distribution of respondents by level of education



Source, Author (2012)

architecture, the study revealed that these were organization objective, security risk, right technology, security policies, operation risk management and the benefits of the adoption of business information security.

Table 3: Respondents opinion on functions of EISA

	Mean	Std deviation
Preventive functions attempt to avoid the occurrence of unwanted events	1.700	683
Detective functions attempt to identify unwanted events during they are occurring or after they have occurred	1.800	.737
Deterrent controls are intended to discourage individuals from intentionally violating information security policies or procedures	1.700	.703
Recovery controls restore lost computing resources or capabilities and help the organization recover monetary losses caused by a security violation	2.450	584
Corrective controls either remedy the circumstances that allowed the unauthorized activity or return conditions to what they were before the violation	1.650	592

Source, Author (2012)

On the finding on various functions of enterprise information security architecture, the study found that respondents agreed that corrective controls either remedy the circumstances that allowed the unauthorized activity or return conditions to what they were before the violation as shown by mean of 1.65, deterrent controls are intended to discourage individuals from intentionally violating information security policies or procedures and preventive functions attempt to avoid the occurrence of unwanted events as shown by mean of 1.7 in each case , detective functions attempt to identify unwanted events when they are occurring or after they have occurred as shown by mean of 1.8 and recovery controls restore lost computing resources or capabilities and help the organization recover monetary losses caused by a security violation as shown by mean of 2.45.

4.4 Model for Adoption of Information Security Architecture

Table 4: Influence of Perceived Environmental Uncertainty on the adoption EISA

	Mean	Std deviation
Unpredictability of major trends or risks in the business environment influence the adoption of information security Architecture	1.860	.683
Possible security risks induced by the emerging technologies that organizations deploy to enhance operational efficiency and effectiveness influence the adoption of information security Architecture	1.992	.738
There is relationship between environmental uncertainty and adoption information security Architecture	2.051	706
Rapid technological development in network and mobile technologies in Kenya has posed a challenge to ensure the confidentiality and availability of information thus need for adoption of information security Architecture	1.639	.584
The greater the level of environmental uncertainty perceived by an organization, the greater the likelihood that the organization will conform to institutional pressures to adopt information security Architecture	1.720	.545

Source, Author (2012)

From the findings on the influence of Perceived Environmental Uncertainty on the adoption of information security Architecture, it was found that rapid technological development in network and mobile technologies in Kenya has posed a challenge to ensure the confidentiality and availability of information thus need for adoption of information security Architecture as shown by mean of 1.639, the greater the level of environmental uncertainty perceived by an organization, the greater the likelihood that the organization will conform to institutional pressures to adopt information security Architecture as shown by mean of 1.720, unpredictability of major trends or risks in the business environment influence the adoption of information security Architecture as shown by mean of 1.860, possible security risks induced by the emerging technologies that organizations deploy to enhance operational efficiency and effectiveness influence the adoption of information security Architecture as shown by mean of 1.992 and that there exist a relationship between environmental uncertainty and adoption information security Architecture as shown by mean of 2.051.

Table 5: Influence of Perceived Gain in Competitive Advantage on adoption of EISA

	Mean	Std deviation
Firms are more likely to conform to institutional requirements if doing so results in a gain in production economics	1.551	547
In hypercompetitive and globalized business environment, organizations and market participants increasingly find it necessary to deploy signaling strategies to potential customers and business partners that differentiate their products and services from the lower quality	1.511	619
Management investment in effective security Architecture can lead to competitive advantages	1.727	.892
Organization are seeking information security certification to increase customers' confidence in online financial transactions	1 864	.909
The greater the gain in competitive advantage perceived by an organization, the greater the likelihood that the organization will conform to institutional pressures to adopt information security management innovations	2.121	.634

Source, Author (2012)

On the influence of various aspects of Perceived Gain in Competitive Advantage on the adoption of information security Architecture, it was found that in very hypercompetitive and globalized business environment, organizations and market participants increasingly find it necessary to deploy signaling strategies to potential customers and business partners that differentiate their products and services from the lower quality as shown by mean of 1.511, firms are more likely to conform to institutional requirements if doing so results in a gain in production economics as shown by mean of 1.551, there is need for management investment in effective security Architecture can lead to competitive advantages as shown by mean of 1.727 , Organization are seeking information security certification to increase customers' confidence in online financial transactions as shown by mean of 1.864 and that as there is greater gains in competitive advantage perceived by an organization, the greater the likelihood that the organization will conform to institutional pressures to adopt information security management innovations as shown by mean of 2.121.

Table 6: Influence of Availability of Resources on the adoption of EISA

	Mean	Std deviation
Availability of resources to an organization determine whether it can afford innovation	1.713	.869
Availability of resources allow firms to be flexible in investing in additional human resources for administrative innovation as well as in absorbing failure costs	1.808	1.041
Information security architecture is an economic decision to the organization	1.656	.968
Firms with larger resources, ones that can tolerate more risk and engage in larger investments in security management, hence are more likely to conform to institutional pressure	2.205	811

Source, Author (2012)

From the findings on the influence of Availability of Resources on the adoption of information security Architecture, it was revealed that Information security architecture is an economic decision to the organization as shown by mean of 1.656, availability of resources to an organization determine whether it can afford innovation as shown by mean of 1.713 , availability of resources allow firms to be flexible in investing in additional human resources for administrative innovation as well as in absorbing failure costs as shown by mean of 1.808 and firms with larger resources, ones that can tolerate more risk and engage in larger investments in security management, hence are more likely to conform to institutional pressure as shown by mean of 2.205 .

Table 7: Influence of Top Management Support on the adoption of EISA

	Mean	Std deviation
Managerial support is required in the adoption of information security architecture, when coordination and conflict resolution among individuals and units are essential	1.382	.614
The role of top management is much more important in the adoption process of information security architecture	1.702	.673
strong participation of top management results in the implementation of an efficient innovation process and activities intended to assimilate these innovations in the organization	1.698	.685
top management support can lead to a centralized impact from information security architecture in an organization	1.654	.845
The greater the top management support, the stronger the relationship between institutional influences and information security architecture adoption	2.176	1.138

Source, Author (2012)

On the influence of various aspect of top management support on the adoption of information security architecture, it was established that managerial support is required in the adoption of information security architecture, when coordination and conflict resolution among individuals and units are essential as shown by mean of 1.382, top management support can lead to a centralized impact from information security architecture in an organization as shown by mean of 1.654, strong participation of top management results in the implementation of an efficient innovation process and activities intended to assimilate these innovations in the organization as shown by mean of 1.698 , the role of top management is much more important in the adoption process of information security architecture as shown by mean of 1.702 and the greater the top management support, the stronger the relationship between institutional influences and information security architecture adoption as shown by mean of 2.176.

Table 8: Influence of IT Capability on the adoption of EISA

	Mean	Std deviation
IT capability allows an organization to connect people to people as well as to innovation activities, such as information security management	1.786	.612
IT capability is important when the nature of the innovation is administratively oriented	1.514	.613
With sufficient IT infrastructure, firms can quickly adjust to changing environmental contingencies and facilitate the organizational learning process	1.496	.648
There is positive relationship between business managers' IT competence and the adoption of information security architecture	1.794	.655
The degree of information security maturity should be assessed using a maturity capability perspective.	1.669	.631
The greater an organization's IT capability, the stronger the relationship between institutional influences and information security architecture adoption	1.492	.510

Source, Author (2012)

From the results on the influence of IT Capability on the adoption of information security Architecture, the study found that the greater an organization's IT capability, the stronger the relationship between institutional influences and information security architecture adoption as shown by mean of 1.492, with sufficient IT infrastructure, firms can quickly adjust to changing environmental contingencies and facilitate the

organizational learning process as shown by mean of 1.496, IT capability is important when the nature of the innovation is administratively oriented as shown by mean of 1.514 , the degree of information security maturity should be assessed using a capability perspective as shown by mean of 1.669, IT capability allows an organization to connect people to people as well as people to innovation activities, such as information security management as shown by mean of 1.786 and there is positive relationship between business managers' IT competence and the adoption of information security architecture as shown by mean of 1.794.

Table 9: Influence of Cultural Acceptability on the adoption of EISA

	Mean	Std deviation
Cultural acceptability plays an equally vital role in supporting the creation of a security culture and the enhancement of employees' security awareness during the adoption of information security architectures	1 547	.701
Competence to maintain policy flexibility, the competence to communicate the necessity for information security procedures, and the competence to facilitate informal communication about information security architecture	2 051	.756
The relationship between institutional influence and the assimilation of information security architectures should be stronger when the cultural acceptability of an innovation is high	2.025	.882

Source, Author (2012)

From the findings on the influence of Cultural Acceptability on the adoption of information security Architecture, the study found that Cultural acceptability plays an equally vital role in supporting the creation of a security culture and the enhancement of employees' security awareness during the adoption of information security architectures as shown by mean of 1.547. There is a relationship between institutional influence and the assimilation of information security architectures should be stronger when the cultural acceptability of an innovation is high as shown by mean of 2.057 and competence to maintain policy flexibility, the competence to communicate the necessity for information security procedures, and the competence to facilitate informal communication about information security architecture as shown by mean of 2.051.

4.5 Factor Analysis

Table 10: Communalities

	Initial	Extraction
Unpredictability of major trends or risks in the business environment influence the adoption of information security Architecture	1.000	.824
Possible security risks induced by the emerging technologies that organizations deploy to enhance operational efficiency and effectiveness influence the adoption of information security Architecture	1.000	737
There is relationship between environmental uncertainty and adoption information security Architecture	1.000	833
Rapid technological development in network and mobile technologies in Kenya has posed a challenge to ensure the confidentiality and availability of information thus need for adoption of information security Architecture	1 000	.752
The greater the level of environmental uncertainty perceived by an organization, the greater the likelihood that the organization will conform to institutional pressures to adopt information security Architecture	1.000	819
Firms are more likely to conform to institutional requirements if doing so results in a gain in production economics	1.000	823
In hypercompetitive and globalized business environment, organizations and market participants increasingly find it necessary to deploy signaling strategies to potential customers and business partners that differentiate their products and services from the lower quality	1.000	.757
Management investment in effective security Architecture can lead to competitive advantages	1.000	.797
Organization are seeking information security certification to increase customers' confidence in online financial transactions	1 000	695
The greater the gain in competitive advantage perceived by an organization, the greater the likelihood that the organization will conform to institutional pressures to adopt information security management innovations	1.000	.847
Availability of resources to an organization determine whether it can afford innovation	1.000	758
Availability of resources allow firms to be flexible in investing in additional human resources for administrative innovation as well as in absorbing failure costs	1.000	.706
Information security architecture is an economic decision to the organization	1.000	.821
Firms with larger resources, ones that can tolerate more risk and engage in larger investments in security management, hence are more likely to conform to institutional pressure	1.000	692
Managerial support is required in the adoption of information security architecture , when coordination and conflict resolution among individuals and units are essential	1.000	.795
The role of top management is much more important in the adoption process of information security architecture	1.000	.792
Strong participation of top management results in the implementation of an efficient innovation process and activities intended to assimilate these innovations in the organization	1.000	.778
Top management support can lead to a centralized impact from information security architecture in an organization	1.000	.734
The greater the top management support, the stronger the relationship between institutional influences and information security architecture adoption	1.000	.895
IT capability allows an organization to connect people to people as well as people to innovation·	1.000	.766

activities, such as information security management		
IT capability is important when the nature of the innovation is administratively oriented	1.000	.872
With sufficient IT infrastructure, firms can quickly adjust to changing environmental contingencies and facilitate the organizational learning process	1.000	.772
There is positive relationship between business managers' IT competence and the adoption of information security architecture	1.000	.737
The degree of information security maturity should be assessed using a capability perspective	1.000	810
The greater an organization's IT capability, the stronger the relationship between institutional influences and information security architecture adoption	1.000	603
Cultural acceptability plays an equally vital role in supporting the creation of a security culture and the enhancement of employees' security awareness during the adoption of information security architectures	1 000	825
Competence to maintain policy flexibility, the competence to communicate the necessity for information security procedures, and the competence to facilitate informal communication about information security architecture	1.000	811
The relationship between institutional influence and the assimilation of information security architectures should be stronger when the cultural acceptability of an innovation is high	1.000	856

Source, Author (2012)

The above table helps the researcher to estimate the communalities for each variance. This is the proportion of variance that each item has in common with other factors. For example 'the greater the top management support, the stronger the relationship between institutional influences and information security architecture adoption' has 89.5% communality or shared relationship with other factors. This value has the greatest communality with others, while 'the greater an organization's IT capability, the stronger the relationship between institutional influences and information security architecture adoption' has the least communality with others of 60.3%.

Table 11: Total Variance Explained

Compone nt	Initial Eigenvalues			Extraction Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	3.831	13.681	13.681	3.831	13.681	13.681
2	3.287	11.741	25.422	3.287	11.741	25.422
3	2.984	10.656	36.078	2.984	10 656	36.078
4	2.697	9.630	45.708	2.697	9.630	45.708
5	2.100	7.501	53.209	2.100	7.501	53.209
6	1.822	6.509	59.718	1.822	6.509	59.718
7	1.602	5.722	65.440	1.602	5.722	65.440
8	1.374	4.907	70.348	1.374	4.907	70 348
9	1.157	4.134	74.481	1 157	4.134	74 481
10	1.052	3.758	78.240	1.052	3.758	78.240
11	.916	3.270	81.510			

12	.853	3.046	84.556			
13	.809	2.888	87.444			
14	.621	2.218	89.662			
15	.536	1.915	91.577			
16	.455	1.624	93.201			
17	.387	1.382	94.583			
18	.315	1.127	95.710			
19	.238	.851	96.560			
20	.216	.772	97.333			
21	.192	.685	98.018			
22	.166	.594	98.612			
23	.123	.440	99.052			
24	.108	.387	99.439			
25	.065	.234	99.673			
26	.040	.145	99.818			
27	.036	.130	99.947			
28	.015	.053	100.000			

In the above table, the researcher used Kaiser Normalization Criterion, which allows for the extraction of components that have an Eigen value greater than 1. The principal component analysis was used and ten factors were extracted. As the table shows, these 10 factors explain 78.24% of the total variation. Factor 1 contributed the highest variation of 13.68%. The contributions decrease as one moves from factor one to the other up to factor ten.

4.6 Regression analysis

Table 12: Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.924	.853	.814	.56743

Adjusted r^2 is called the coefficient of determination and shows how adoption of Enterprise information security architecture varies with Perceived Environmental Uncertainty, Perceived Gain in Competitive Advantage, Availability of Resources, Top Management Support, IT Capability and Cultural Acceptability. From data, the value of adjusted r^2 is 0.814. This implies that there was a variation of 81.4% of adoption of Enterprise information security architecture with changes in Perceived

Environmental Uncertainty, Perceived Gain in Competitive Advantage, Availability of Resources, Top Management Support, IT Capability and Cultural Acceptability at 95% confidence interval. There was a strong positive relationship between adoption of Enterprise information security architecture and Perceived Environmental Uncertainty, Perceived Gain in Competitive Advantage, Availability of Resources, Top Management Support, IT Capability and Cultural Acceptability as shown by correlation coefficient of 0.924.

Table 13: Regression Coefficients

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig
		B	Std. Error	Beta		
1	(Constant)	.044	.195		2.056	.001
	Perceived Environmental Uncertainty	.310	.056	309	1.498	.000
	Perceived Gain in Competitive Advantage	.272	.053	.293	1.159	.000
	Availability of Resources	.031	.061	.032	.507	.013
	Top Management Support	.069	.076	.059	.909	.034
	IT Capability	.308	.078	.246	1.970	.000
	Cultural Acceptability	.247	.084	.197	2.045	.004

From the above results on regression coefficient, it was found that unit increase in Perceived Environmental Uncertainty, Perceived Gain in Competitive Advantage, Availability of Resources, Top Management Support, IT Capability and Cultural Acceptability would lead to increased adoption of information security architecture. From the regression coefficient it was found that Perceived Environmental Uncertainty, had the greatest influence on the adoption of Information security architecture, followed by IT Capability, Perceived Gain in Competitive Advantage, Cultural Acceptability, Top Management Support and Availability of Resources.

Hypothesis Testing

The critical value established from the distribution table at 5% significance level and 19 degrees of freedom was 2.093

Hypothesis 1: *The greater the level of environmental uncertainty perceived by an organization, the greater the likelihood that the organization will conform to*

institutional pressures; peer influence and supervisory authority influence to adopt information security Architecture innovations.

On comparing the critical value and the calculated value (1.498 < 2.093) the calculated value is less than the critical value, this leads to the acceptance of the hypothesis that the greater the level of environmental uncertainty perceived by an organization, the greater the likelihood that the organization will conform to institutional pressures; peer influence and supervisory authority influence to adopt information security Architecture innovations.

Hypothesis 2: *The greater the gain in competitive advantage perceived by an organization, the greater the likelihood that the organization will conform to institutional pressures peer influence and supervisory authority influence to adopt information security Architecture innovations.*

On comparing the critical value and the calculated value (1.159 < 2.093) the calculated value is less than the critical value, this leads to the acceptance of the hypothesis that the greater the gain in competitive advantage perceived by an organization, the greater the likelihood that the organization will conform to institutional pressures peer influence and supervisory authority influence to adopt information security Architecture innovations.

Hypothesis 3: *The greater the availability of organizational resources, the greater the likelihood that the organization will conform to institutional pressures peer influence and supervisory authority influence to adopt information security Architecture innovations.*

On comparing the critical value and the calculated value (0.507 < 2.093) the calculated value is less than the critical value, this leads to the acceptance of the hypothesis that the greater the availability of organizational resources, the greater the likelihood that the organization will conform to institutional pressures peer influence

and supervisory authority influence to adopt information security Architecture innovations.

Hypothesis 4: *The greater the top management support, the stronger the relationship between institutional influences peer influence and supervisory authority influence and information security Architecture adoption.*

On comparing the critical value and the calculated value (0.909 < 2.093) the calculated value is less than the critical value, this leads to the acceptance of the hypothesis that the greater the top management support, the stronger the relationship between institutional influences peer influence and supervisory authority influence and information security Architecture adoption.

Hypothesis 5: *The greater an organization's IT capability, the stronger the relationship between institutional influences peer influence and supervisory authority influence and information security Architecture adoption.*

On comparing the critical value and the calculated value (1.907 < 2.093) the calculated value is less than the critical value, this leads to the acceptance of the hypothesis that the greater an organization's IT capability, the stronger the relationship between institutional influences peer influence and supervisory authority influence and information security Architecture adoption.

Hypothesis 6: *The higher the cultural acceptability of innovation, the stronger the relationship between institutional influences peer influence and supervisory authority influence and information security Architecture adoption.*

On comparing the critical value and the calculated value (2.045 < 2.093) the calculated value is less than the critical value, this leads to the acceptance of the hypothesis that the higher the cultural acceptability of innovation, the stronger the

relationship between institutional influences peer influence and supervisory authority influence and information security Architecture adoption.

All the hypotheses were found to be statistically significant as the significance values were less than 0.05, an indication that the data used was statistically significant to make conclusions for the study.

4.7 Correlations Analysis

Table 14: Correlations

		Adoption of EISA	Perceived Environmental Uncertainty	Perceived Gain in Competitive Advantage	Availability of Resources	Top Management Support	IT Capability	Cultural Acceptability
Adoption of EISA	Pearson Correlation	1	668**	.5275**	.543	.715**	.608**	.371
	Sig. (2-tailed)		.000	.000	.000	.059	.075	.005
	N	272	272	272	272	272	272	272
Perceived Environmental Uncertainty	Pearson Correlation	.668**	1	.107	.327**	-.014	.293	-.080**
	Sig. (2-tailed)	.000		.079	.000	.815	.000	186
	N	272	272	272	272	272	272	272
Perceived Gain in Competitive Advantage	Pearson Correlation	.575**	.107	1	.009**	.478	-.026	.184**
	Sig. (2-tailed)	.000	.079		.878	000	.670	.002
	N	272	272	272	272	272	272	272
Availability of Resources	Pearson Correlation	.543**	.327**	.009	1**	.053**	.577	.225**
	Sig. (2-tailed)	.000	.000	.878		.381	.000	000
	N	272	272	272	272	272	272	272
Top Management Support	Pearson Correlation	.715	-.014	.478**	.053	1	.258**	.206
	Sig. (2-tailed)	.059	815	.000	.381		.000	.001
	N	272	272	272	272	272	272	272
IT Capability	Pearson Correlation	.608	.293**	-.026	.577	.258**	1	.232
	Sig. (2-tailed)	.075	.000	.670	.000	.000		.000
	N	272	272	272	272	272	272	272
Cultural	Pearson	.371**	-.080	.184**	.225**	.206	.232**	1**

Acceptability	Correlation							
	Sig. (2-tailed)	005	186	.002	.000	.001	000	
	N	272	272	272	272	272	272	272

From the correlation results it was found that Perceived Environmental Uncertainty, Perceived Gain in Competitive Advantage, Availability of Resources, Top Management Support, IT Capability and Cultural Acceptability had positive strong relationship with adoption of Information security architectures as shown by positive correlation coefficient which were found to be statistically significant except for cultural acceptability and availability of resources, which were found not to be significant but were positively associated with adoption of Information security architecture.

CHAPTER FIVE:
SUMMARY OF FINDINGS CONCLUSIONS AND RECOMMENDATIONS

5.1 Findings

This study established information security architecture as an administrative innovation that can be adopted to manage information security risks and vulnerabilities. The data we collected provide strong support that management styles and interpretations influence the information security best practices adopted by the organization. The study shows that an institution's policies have a significant influence on adoption and assimilation of information security architecture innovations.

5.1.1 Summary of Findings

Table 15 summarizes the results of our hypothesis testing. Our findings are consistent with prior studies.

Table 15: Summary of Findings

	Hypothesis	Result
H1	The greater the level of environmental uncertainty perceived by an organization, the greater the likelihood that the organization will conform to institutional pressures; peer influence and supervisory authority influence to adopt information security Architecture innovations.	Supported
H2	The greater the gain in competitive advantage perceived by an organization, the greater the likelihood that the organization will conform to institutional pressures peer influence and supervisory authority influence to adopt information security Architecture innovations.	Supported
H3	The greater the availability of organizational resources, the greater the likelihood that the organization will conform to institutional pressures peer influence and supervisory authority influence to adopt information security Architecture innovations.	Supported
H4	The greater the top management support, the stronger the relationship between institutional influences peer influence and supervisory authority influence and information security Architecture adoption.	Supported
H5	The greater an organization's IT capability, the stronger the relationship between institutional influences peer influence and supervisory authority influence and information security Architecture adoption	Supported
H6	The higher the cultural acceptability of innovation, the stronger the relationship between institutional influences (a) peer influence and (b) supervisory authority influence and information security architecture adoption	Supported

5.1.2 Moderating Variables

(a) Perceived Environment Uncertainty

The organizations we interviewed emphasized the importance of this factor at the adoption stage.

(b) Perceived Gain in Competitive Advantage

The organizations interviewed believe that adoption of information security architecture allowed the organization to generate more business opportunities than other firms.

(c) Availability of Resources

The organizations we interviewed consistently emphasized that the availability of resources is particularly important when organizations are considering to what extent they will fully invest in EISA, even when the potential return is unclear.

(d) Top Management Support

As widely expected, the organizations we interviewed confirmed that the tone at the top was a critical element in order to achieve innovation assimilation. Also the results clearly showed that top management support increased the effectiveness of information security.

(e) IT Capability

As widely discussed in the literature, the results confirmed the crucial role of IT in the assimilation process as most organizations managed their innovations through IT infrastructures.

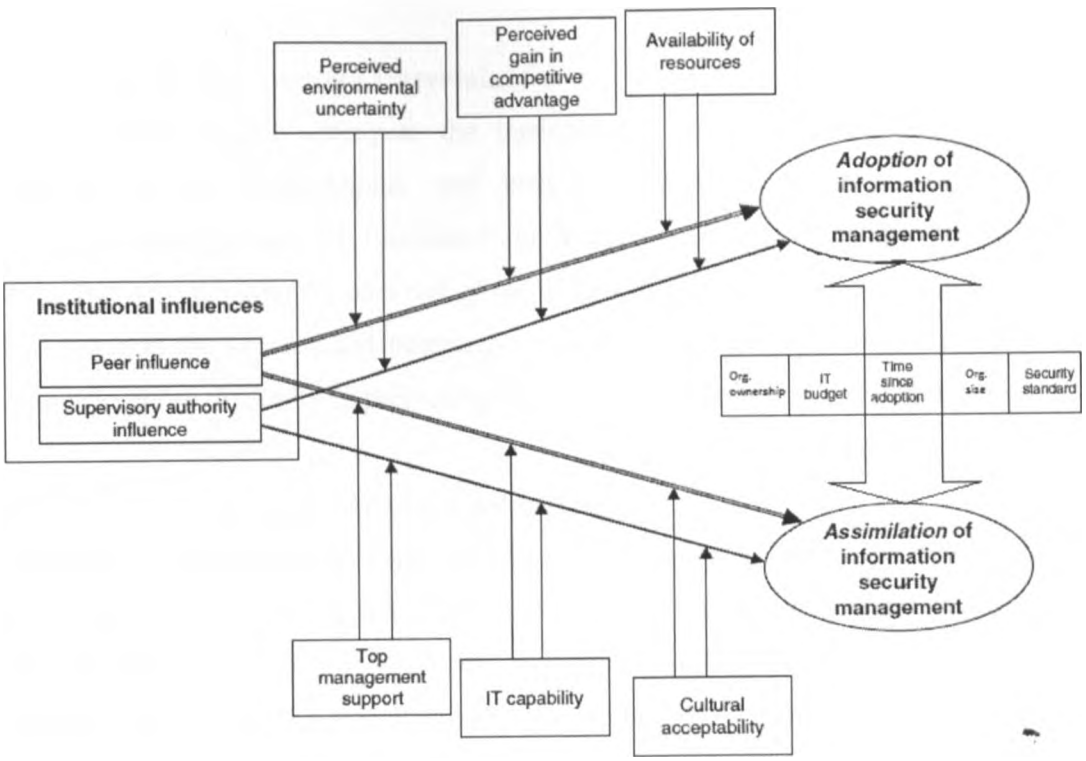
(f) Cultural Acceptability

This came out as a very strong factor indicating that cultural change is critical for successful assimilation. This means that diffusion of administrative innovation in an organization is a social activity.

5.2 Proposed Methodology for Adoption and Assimilation of EISA in the Oil and Gas Industry

Figure 6: The suggested methodology suitable for adoption of Information security architecture in Oil and Gas Industry in Kenya was derived from the literature, survey of the Oil and Gas industry IS managers, interaction with theory of innovation diffusion and the Study carried out on major Oil and Gas companies in Kenya.

Figure 6: Proposed Methodology for Adoption of Information Security Architecture



Components of the Framework

5.2.1 Institutional Influence

(a) Peer Influence

Most successful peer firms adopt one or more frameworks for information security architecture. An organization should draw from the experiences of successful peer

firms in investigating and implementing information security architecture frameworks.

(b) Supervisory Authority Influence

Supervisory regulators should be in the forefront as proponents of information security architecture. Supervisory regulators may pressure enterprises to investigate and to undertake the organization's information security architecture implementation programs.

5.2.2 Economic Based Moderating Variables

(a) Perceived Environment Uncertainty

Organizations cannot anticipate the business and computer risks resulting from changes in the technological and business environments. It is difficult for organizations to foresee the likelihood and determine the impact of potential security risks that may threaten the survival of the organization. Organizations cannot identify and interpret the sources and potential consequences of environmental volatility and may have more difficulty in predicting business and technological obsolescence.

(b) Perceived Gain in Competitive Advantage

Adoption of information security Architecture makes the organization more efficient and allows organization to manage resources better than other firms. Furthermore, the adoption of information security architecture makes business processes more efficient and allows the organization to generate more business opportunities than other firms.

(c) Availability of Resources

In the adoption of EISA, organizations need more human resources that will be used for information security architecture. Organization should have more flexible infrastructure to efficiently support information security Architecture. Organization should have more efficient and streamlined business processes that can result in successful adoption of information security architecture.

5.2.3 Organizational Capability Based Moderating Variables

(a) Top Management Support

Senior management of organizations should demonstrate support for information security architecture. Senior management of organization should formulate a strategy for the introduction of information security architecture. Top management should also establish processes and standards to monitor information security architecture adoption and be involved in the decision-making process.

(b) IT Capability

There is need for organizations to have strong IT leadership, IT planning capability, enough experience with IT, competent IT staff and perceive the importance of strategic use of IT. Budgetary allocations is highly dependent on support from executive management hence the need for them to buy into the innovation.

(c) Cultural Acceptability

There is need for organizations commitment to innovation and change. Organizations should be willing to take risks, emphasize growth through acquiring new resources and standards, be dynamic to be first with competitive actions, outcomes and achievements and willing to change formal rules and policies.

5.2.4 Adoption and Assimilation

(a) Adoption of Information Security Architecture

Organizations should consider the adoption of information security Architecture as a means to achieve information protection, confidentiality, integrity and availability.

(b) **Assimilation of Information Security Architecture**

There is need for organizations to establish a security policy, objectives, targets, and processes relevant to managing risks and improving information security in order to deliver results in accordance with the organization's overall policies and objectives. Organizations should implement and operate information security, policy, controls,

and processes and assess and measure process performance against security policy, objectives and practical experience and report the results to management for review. Organizations should take corrective and preventive actions based on the results of the management review to achieve continual improvement of information security Architecture. Increased organizational security effectiveness is attained by implementing information security Architecture in a more integrated manner to support higher levels of organizational work.

5.3 Conclusion

The researcher had intended to understand the conditions that shape the diffusion of an information security administrative innovation, to examine the institutional effects occurring at different stages of innovation adoption and assimilation and to determine the moderators of institutional conformity during each stage of information security Architecture adoption and assimilation. As a result, the study has successfully developed a methodology for adoption and assimilation of information security architecture as an administrative innovation.

Table 16: Mapping Objectives into Research Questions

	Objectives	How they were achieved
1	To determine the impact of institutional influences in the adoption and assimilation of information security architecture as an administrative innovation;	Literature review/personal interviews, Questionnaires
2	To ascertain the effects of institutional influences at different stages of adoption and assimilation;	Literature review, personal interviews, Questionnaires,
3	To examine the moderating economic and organizational factors in the adoption and assimilation of information security architecture.	Literature review, personal interviews, Questionnaires,

The results of this study provide evidence that the development of regulation in different countries does have an impact on the adoption and assimilation of information security management. The findings indicate that at the outset of information security architecture innovation, supervisory authority can play a significant role in stimulating and enforcing the adoption and assimilation of this new management practice. This can offer some encouraging evidence for regulators to evaluate the effectiveness of rules and regulations on corporate governance. The results here can also serve as a positive indicator for other countries where information security architecture is still in its infancy. Findings also indicate that establishment of regulations or guidelines on data protection and governance and increased awareness of regulations are mechanisms that encourage better security and educate organizations about its benefits. Alternatively, given the positive results of mimetic force in our study, there is the practical implication that the regulatory authority can work with leading institutions in initiating information security management. This will be particularly effective where the marketplace is hypercompetitive and there is high uncertainty.

Furthermore, the results demonstrate that whereas external influences are key to good organizational decisions about adoption and assimilation of information security Architecture practices, adoption was moderated by the economic evaluation of the business environment and assimilation was moderated by internal organizational capabilities. Therefore, firms can more effectively diffuse information security practices when they give voice to and make sound business cases for the economic value of security.

By proactively evaluating economic conditions, managers can make timely strategic responses to institutional pressure to conform when adopting information security innovations. Being more aware of environmental uncertainty, competitive pressures, and the availability of resources, for instance, gives managers insight into how to successfully adopt an information security architecture framework. As a result, with timely adoption, firms are more likely to avoid risks and the consequent costs associated with information security breaches.

In the assimilation stage, study shows that top management support, IT capabilities, and cultural acceptability play crucial roles in ensuring that information security management practices become embedded in organizational practices. A sound and effective information security management requires the support of top management and organizational culture. To demonstrate top management support, we consider that the establishment of a CISO role can serve as a strong signal in the commitment of senior management to security. Furthermore, our work reiterates the importance of culture in assimilating information security Architecture in organizations.

5.4 Recommendations

Three critical economic factors were identified: environmental uncertainty, competitive advantages, and availability of resources. Indeed, these factors have been discussed in previous research on information security adoption and effectiveness. From an organizational capability perspective, three important factors were derived

including top management support, IT capability and cultural these factors were also mentioned most frequently as key organizational capability factors in prior studies.

5.4.1 Environmental uncertainty

Every organization that we interviewed emphasized the importance of this in the adoption stage. When decision-makers fail to acknowledge or misinterpret the sources and potential consequences of environmental uncertainties related to information security management, the impact can be a serious decline in an organization's performance or damage to its legitimacy in the institutional environment.

5.4.2 Competitive Advantage

Another important concern consistently emphasized by interviewees was economic benefits. In the rapidly changing business environment, organizations need to create a competitive advantage to differentiate their products and services. Investment in information security can generate competitive advantages because of a stronger corporate image and enhanced customer confidence.

5.4.3 Availability of Resources

From our interviews, we realized that available resources allow firms to fund an innovation, absorb the cost of unsuccessful implementation, and implement the innovation by exploring new ideas. Therefore, the availability of resources is particularly important when organizations consider to what extent they will fully invest in information security management, a simple policy document or a full-scale enterprise implementation.

5.4.4 Top Management Support

All interviewees pointed out that top management support is a critical element of any successful innovation assimilation. Studies in information security Architecture also show that top management support has a positive impact on increasing security effectiveness.

5.4.5 IT Capability

As most interviewees mentioned, an organization manages its innovations through IT infrastructure, that is to say a framework that connects different members of the organization with internal and external knowledge and processes. The usefulness and roles of IT in the assimilation process have been widely discussed in the literature.

5.4.6 Cultural (Organizational Culture) Acceptability

This factor was strongly and consistently recommended by all interviewees. Since diffusing administrative innovation in an organization is as much a social activity as it is a managerial and/or technical activity, cultural change is a prerequisite for its successful assimilation.

5.5 Limitations of the Study and Suggestions for Future Research

In the process of conducting this Study, we encountered a number of limitions some of which offer opportunities for future research. The duration of the Study was not long enough to enable a proper investigation of the responses and survey all the existing Oil and Gas companies, therefore the results may suffer from internal validity threats. Majority of the respondents were managers in ICT department who may not have the final authority in making decsions to adopt information security architecture. Since the study is solely conducted on major oil and gas companies in Kenya, the results may suffer from regional and industry biases. Therefore the results needs to be interpreted carefully and replicated in other industry and countries to improve their relevance.

The results of this study suggest new directions for future research. Researchers in the field of information security architecture ought to put more emphasis on adoption and assimilation of information security architecture as an administrative innovation rather than as a technological innovation. Furthermore, an indepth study is required to rationalize the moderating factors.

REFERENCES

Agarwal, R., Prasa, J. (1998), "A conceptual and operational definition of personal innovativeness in the domain of information technology", *Information Systems Research*, Vol. 9 No.2, pp.204-301.

Agarwal, R., Sambamurthy, V., Stair, R. (2000), "The evolving relationship between general and specific computer self-efficacy: an empirical assessment", *Information Systems Research*, Vol. 11 No.4, pp.418-30.

Ajzen, I. (1991), "The theory of planned behavior", *Organizational Behavior and Human Decision Processes*, Vol. 50 No.2, pp.179-211.

Ajzen, I., Madden, T.J. (1986), "Prediction of goal-directed behavior: attitudes, intentions, and perceived behavioral control", *Journal of Experimental Social Psychology*, Vol. 22 pp.453-74.

Anderson, K (2008). A Business Model for Information Security. Information Systems Control Journal, vol. 3, 51-52.

Anil, S., Ting, L.T., Moe, L.H., Jonathan, G.P.G. (2003), "Overcoming barriers to the successful adoption of mobile commerce in Singapore", *International Journal of Mobile Communications*, Vol. 1 No.1/2, pp.194-231.

BS 7799-2 (1999), Information Security Management Part 2: Specification for Information Security Management Systems, British Standards Institute, London.

COBIT (1998), COBIT: Control Objectives, ISACA, Rolling Meadows, IL.

Davis, F.D. (1989), "Perceived usefulness, perceived ease of use and user acceptance of information technology", *MIS Quarterly*, Vol. 13 No.3, pp.319-40.

Davis, F.D., Bagozzi, R.P., Warshaw, P.R. (1989), "User acceptance of computer technology: a comparison of two theoretical models", *Management Science*, Vol. 35 No.8, pp.982-1003.

Flynn, N.L. (2001), The Epolicy Handbook: Designing and Implementing Effective E-mail, Internet and Software Policies, American Management Association, New York, NY.

Fred Cohen (2006). Enterprise Information Protection, New York Press, USA.

Fred Cohen (2006). Security Governance Checklists: Business Operations, Security Governance, Risk Management, and Enterprise Security Architecture, New York Press, USA.

Gartner. "Incorporating Security into the Enterprise Architecture Framework".

Ghosh, A.K., Swaminatha, T.M. (2001), "Software security and privacy risks in mobile e-commerce", *Communications of the ACM*, Vol. 44 No.2, pp.51-7.

Gollmann, D. (1999), Computer Security, John Wiley & Sons, New York, NY.

Gupta, M., Charturvedi, A.R., Metha, S., Valeri, L. (2001), "The experimental analysis of information security management issues for online financial services", ICIS 2000, pp.667-75.

Hulland, J.S. (1999), "Use of partial least squares (PLS) in strategic management research: a review of four recent studies", *Strategic Management Journal*, Vol. 20 No.2, pp.195-204.

Hsu, C., Lee JN., Straub, DW. (2009), "Institutional Influences on Information Systems Security Innovations", Articles in Advance 2012, pp.1-22.

ISO/IEC 17799 (2000), Information Technology Code of Practice for Information Services, International Organization for Standardization, Geneva.

J. A. (1987). A Framework for Information Systems Architecture. IBM Systems Journal, vol. 26, no. 3, IBM Publication G321-5298.

Kabay, M.E. (1996), The NCSA Guide to Enterprise Security, McGraw-Hill, New York, NY,

Kalakota, R., Robinson, M. (2002), *M-business: The Race to Mobility*, McGraw-Hill, New York, NY.

Kiely, L. & Benzel T. (2006). Systemic Security Management: A New Conceptual Framework for Understanding the Issues, Inviting Dialogue and Debate, and Identifying Future Research Needs. Institute for Critical Information Infrastructure Protection (ICIIP), University of Southern California Marshall School of Business, USA.

Lee, S.M., Luthans, F., Olson, D.L. (1982), "A management science approach to contingency models of organizational structure", Academy of Management Journal, Vol. 25 No.3, pp.553-66.

Lee, Y.E., Benbasat, I. (2003), "Interface design for mobile commerce", *Communications of the ACM*, Vol. 46 No.12, pp.49-52.

Limayem, M., Khalifa, M., Frini, A. (2000), "What makes consumers buy from internet? A longitudinal study of online shopping", *IEEE Transactions on Systems, Man and Cybernetics Part A: Systems and Humans*, Vol. 30 No.4, pp.421-32.

Mallat, N., Rossi, M., Tuunainen, V.K., Öörni, A. (2006), "The impact of use situation and mobility on the acceptance of mobile ticketing services", *Proceedings of the 39th Annual Hawaii International Conference on System Sciences*, IEEE Computer Society Press, New York, NY, .

Marakas, M.Y., Yi, Y., Johnson, R.D. (1998), "The multilevel and multifaceted character of computer self-efficacy: toward clarification of the construct and an integrative framework for research", *Information Systems Research*, Vol. 9 No.2, pp.126-63.

Michelle S., Huirong F., Zhu Y. (2009). Enterprise Information Security Architecture, A Review of Frameworks, Methodology and Case Studies, ©2009 IEEE

Robbins, S.P. (1994), Management, 4th ed., Prentice-Hall, Upper Saddle River, NJ.

Schultz, E.E., Proctor, R.W., Lien, M.C. (2001), "Usability and security: an appraisal of usability issues in information security methods", Computers & Security, Vol. 20 No.18, pp.620-34.

Sherwood J., Clark A., Lynas D. (2008). Enterprise Security Architecture, A Business-drive model for Security, January 2008, http://www.sabsa.org/the-sabsa-method.aspx

Sherwood, J. (1996), "SALSA: a method for developing the enterprise security architecture and strategy", Computers & Security, Vol. 2 pp.8-17.

Simson, G., Gene, S. (1991), Practical UNIX Security, O'Reilly & Associates, Sebastopol, CA.

Tudor, J.K. (2001), Information Security Architecture, CRC Press, Boca Raton, FL.

Venkatesh, V. (2000), "Determinants of perceived ease of use: integrating control, intrinsic motivation, and emotion into the technology acceptance model", *Information Systems Research*, Vol. 11 No.4, pp.342-65.

Venkatesh, V., Davis, F.D. (1996), "A model of the antecedents of perceived ease of use: development and test", *Decision Sciences*, Vol. 27 No.3, pp.451-81.

Venkatesh, V., Davis, F.D. (2000), "A theoretical extension of the technology acceptance model: four longitudinal field studies", *Management Science*, Vol. 46 No.2, pp.186-204.

Von Solms, R., Van Haar, H., Von Solms, S.H., Caelli, W.J. (1994), "A framework for information security evaluation", Information & Management, Vol. 26 No.3, pp.143-53.

Weber, R. (1999), Information System Control and Audit, Prentice-Hall, Englewood Cliffs, NJ.

Wu, J.H., Wang, S.C. (2005), "What drives mobile commerce? An empirical evaluation of the revised technology acceptance model", *Information & Management*, Vol. 42 No.5, pp.719-29.

APPENDICES

Appendix I: Introductory Letter

To: .....

Dear Respondent

REF: REQUEST FOR RESEARCH DATA COLLECTION

I am a Master of Science in Information Systems, student at the University of Nairobi and currently conducting a research on **A Methodology for Adoption and Assimilation of Enterprise Information Security Architecture: Case Study in the Oil & Gas Industry**. You have been identified as a potential respondent in this study owing to your strategic position in providing the most reliable information on the same. Please respond to all questions as appropriate either by tick or writing your answer on the space provided using you best estimates. This is an academic research and the answers you supply will be treated in utmost confidence and propriety.

Thank you for your co-operation,

Yours Faithfully,

DANIEL K. SIGEI

P56/70452/2007

Appendix II: Questionnaire

Instructions

Kindly answer all questions by ticking or explaining as appropriate as per your opinion and based on the facts. Where possible you can quote figures.

GENERAL INFORMATION

1. Name of the company .....
2. How long have you served in the company?

   Less than 1year [ ]
   2 to 5 years [ ]
   5 to 10 years [ ]
   More than 10 years [ ]

3. What is your gender?

   Male [ ]
   Female [ ]

4. What is your age bracket?

   Below 25 years [ ]
   25 to 35 years [ ]
   35 to 45 years [ ]
   45 to 55 years [ ]
   Above 55 years [ ]

5. What is your level of education? (Tick where appropriate)

   PhD [ ]
   Master [ ]
   Bachelors [ ]
   Diploma or equivalent [ ]

6. Has your company adopted an Enterprise Information Security Architecture?

   Yes [ ] No [ ]

Section B: Adoption of Enterprise Information Security Architecture

7. What is the organizations strategy and structure in the adoption of Enterprise Information Security?

.....

.....

.....

8. To what extent does the following factors affect the adoption of Enterprise Information Security?

	Very great extent	Great extent	Moderate	Less extent	Not at all
Conceptual security architecture					
Logical security architecture					
Physical security architecture					
Component security architecture					
Operation security architecture					

9. What are the various business requirements in the adoption of enterprise information security architectures?

.....

.....

.....

10. What are the models used in the adoption of enterprise information security architecture?

.....

.....

.....

11. In the adoption of enterprise information security architecture which are the various controls put in place by the organization?

.....

.....

.....

12. To what extent do you agree with the following as functions of enterprise information security architecture?

	Strongly agree	Agree	Moderate	Disagree	Strongly disagree
Preventive functions attempt to avoid the occurrence of unwanted events					
Detective functions attempt to identify unwanted events during they are occurring or after they have occurred					
Deterrent controls are intended to discourage individuals from intentionally violating information security policies or procedures					
Recovery controls restore lost computing resources or capabilities and help the organization recover monetary losses caused by a security violation					
Corrective controls either remedy the circumstances that allowed the unauthorized activity or return conditions to what they were before the violation					

13. Which are the various risk analysis process used by your organization in the adoption of enterprise information security architecture?

.....

.....

.....

.....

14. Which are the various operation risks considered in the adoption of enterprise information security architecture?

.....

.....

.....

.....

Section C: Framework for Implementation of Information Security Architecture

Perceived Environmental Uncertainty

15. To what extent do you agree with the influence of various aspect of Perceived Environmental Uncertainty on the adoption of information security Architecture?

	Strongly agree	Agree	Moderate	Disagree	Strongly disagree
Unpredictability of major trends or risks in the business environment influence the adoption of information security Architecture					
Possible security risks induced by the emerging technologies that organizations deploy to enhance operational efficiency and effectiveness influence the adoption of information security Architecture					

There is relationship between environmental uncertainty and adoption information security Architecture					
Rapid technological development in network and mobile technologies in Kenya has posed a challenge to ensure the confidentiality and availability of information thus need for adoption of information security Architecture					
The greater the level of environmental uncertainty perceived by an organization, the greater the likelihood that the organization will conform to institutional pressures to adopt information security Architecture					

Perceived Gain in Competitive Advantage

16. To what extent do you agree with the influence of various aspect of Perceived Gain in Competitive Advantage on the adoption of information security Architecture?

	Strongly agree	Agree	Moderate	Disagree	Strongly disagree
Firms are more likely to conform to institutional requirements if doing so results in a gain in production economics					
In hypercompetitive and globalized business environment, organizations and market participants increasingly find it necessary to deploy signaling strategies to potential customers and business partners that differentiate their products and services from the lower quality					
Management investment in effective security Architecture can lead to competitive advantages					
Organization are seeking information security certification to increase customers' confidence in online financial transactions					
The greater the gain in competitive advantage perceived by an organization, the greater the likelihood that the organization will conform to institutional pressures to adopt information security management innovations					

Availability of Resources

17. To what extent do you agree with the influence of various aspect of Availability of Resources on the adoption of information security Architecture?

	Strongly agree	Agree	Moderate	Disagree	Strongly disagree
Availability of resources to an organization determine whether it can afford innovation					
Availability of resources allow firms to be flexible in investing in additional human resources for administrative innovation as well as in absorbing failure costs					
Information security architecture is an economic decision to the organization					

Firms with larger resources, ones that can tolerate more risk and engage in larger investments in security management, hence are more likely to conform to institutional pressure					

Top Management Support

18. To what extent do you agree with the influence of various aspect of Top Management Support on the adoption of information security Architecture?

	Strongly agree	Agree	Moderate	Disagree	Strongly disagree
Managerial support is required in the adoption of information security architecture , when coordination and conflict resolution among individuals and units are essential					
The role of top management is much more important in the adoption process of information security architecture					
Strong participation of top management results in the implementation of an efficient innovation process and activities intended to assimilate these innovations in the organization					
Top management support can lead to a centralized impact from information security architecture in an organization					
The greater the top management support, the stronger the relationship between institutional influences and information security architecture adoption					

IT Capability

19. To what extent do you agree with the influence of various aspect of IT Capability on the adoption of information security Architecture?

	Strongly agree	Agree	Neutral	Disagree	Strongly disagree
IT capability allows an organization to connect people to people as well as people to innovation activities, such as information security management					
IT capability is important when the nature of the innovation is administratively oriented					
With sufficient IT infrastructure, firms can quickly adjust to changing environmental contingencies and facilitate the organizational learning process					
There is positive relationship between business managers' IT competence and the adoption of information security architecture					
The degree of information security maturity should be assessed using a capability perspective					
The greater an organization's IT capability, the stronger the relationship between					

institutional influences and information security architecture adoption					

Cultural Acceptability

20. To what extent do you agree with the influence of various aspect of Cultural Acceptability on the adoption of information security Architecture?

	Strongly agree	Agree	Neutral	Disagree	Strongly disagree
Cultural acceptability plays an equally vital role in supporting the creation of a security culture and the enhancement of employees' security awareness during the adoption of information security architectures					
Competence to maintain policy flexibility, the competence to communicate the necessity for information security procedures, and the competence to facilitate informal communication about information security architecture					
The relationship between institutional influence and the assimilation of information security architectures should be stronger when the cultural acceptability of an innovation is high					

Thank you for your time

Appendix III: List of Oil and Gas Companies in Kenya (Sampling Frame)

Name of Oil and Gas company	% Market Share	Position
1. Hashi Energy Ltd	1.7	
2. Kenol kobil Ltd	24.8	1
3. Mul Oil Kenya Limited	0.2	
4. Kenya Shell Limited	19	2
5. Oil Libya Kenya Limited	8.5	5
6. National Oil Corporation Of Kenya	4.6	6
7. Total Kenya Limited	17.9	3
8. Al Leyl Kenya Limited	0.2	
9. Petro Kenya Limited	0.4	
10. Bakri International Energy Co. (K) Ltd	2.4	
11. Chevron Oil Kenya Limited	11.2	4
12. MGS Company Limited	0.7	
13. Fossil Kenya Limited	0.8	
14. Rivapet Kenya Limited	0.9	
15. Engen Kenya Limited	1.2	
16. Oil Com Kenya Limited	1.8	
17. Gapco Kenya Limited	3.8	
Total	100.0	

Source: Annual report, 2009

Appendix IV: Profile of the Sample

Total Sales Revenue

Name of Oil and Gas company	Sales Revenue Kshs m
Kenya Shell Limited	23,233
Total Kenya Limited	16,000
National Oil Corporation Of Kenya	5,367
KenolKobil Ltd	35,198
Oil Libya Kenya Limited	8,456

Source: Annual report, 2011

IT Budget as a % of total sales:

Name of Oil and Gas company	Amount Kshs million	% total revenue
Kenya Shell Limited	30	0.13
Total Kenya Limited	20	0.13
National Oil Corporation Of Kenya	7	0.13
KenolKobil Ltd	40	0.11
Oil Libya Kenya Limited	17	0.20

Information Security Practice Adopted:

Name of Oil and Gas company	Security Management Practices	Security Architecture Practices
Kenya Shell Limited	ISO/IEC 27002/COBIT	Undocumented
Total Kenya Limited	ISO/IEC 27002	Undocumented
NOCK	ISO/IEC 27002	Undocumented
KenolKobil Ltd	ISO/IEC 27002/COBIT	Undocumented
Oil Libya Kenya Limited	ISO/IEC 27002	Undocumented

Source: Author