INFORMATION SECURITY MANAGEMENT STRATEGY IMPLEMENTATION CHALLENGES AT KENYA ELECTRICITY GENERATING COMPANY

KATUA FAITH SYOMBUA

A RESEARCH PROJECT SUBMITTED IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE AWARD OF THE DEGREE OF MASTERS IN BUSINESS ADMINISTRATION OF THE UNIVERSITY OF NAIROBI

NOVEMBER, 2014

DECLARATION

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

Signed.. Date...

KATUA FAITH SYOMBUA

D61/79100/2012

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

Signed.. Date...

DR.REGINA KITIABI

LECTURER

DEPARTMENT OF BUSINESS ADMINISTRATION

UNIVERSITY OF NAIROBI

ACKNOWLEDGEMENTS

First and foremost I wish to thank the Almighty God.

My special appreciation goes to my supervisor Dr. Regina Kitiabi for the patience and guidance throughout my project work. Her professional advice was of great inspiration.

I would like to thank the employees at Kenya Electricity Generating Company and the management team who gave me much support in my research work hence enabling successful completion.

I would like to sincerely thank my friend and husband Chumari Wachaga for all the support and encouragement. I also appreciate my mother Priscilah Mukina and father Katua Joel for the effort and sacrifices they made in bringing me up and teaching me the value of education.

Finally I appreciate the rest of the people who assisted me in any other way and have not been mentioned above.

DEDICATION

This research project is dedicated to my family and friends. Thank you for the love, support and always being there for me. God bless you.

ABSTRACT

The value of information goes beyond the written words and numbers: knowledge, concepts, ideas and brands are examples of intangible forms of information. Information security is achieved by implementing a suitable set of controls, including policies, processes, procedures, organizational structures, software and hardware functions. Security is about managing risk, and risk management covers opportunity and threat. The objectives of this study were: to establish drivers of the information security strategy implementation in KenGen and to establish the challenges in information security strategy implementation in KenGen. The research was conducted through a case study. Primary data was collected for the study using the interview method. The focus was on top management who are the key people involved in strategic decisions. The content analysis technique was used to analyze the data. The study concludes that there were several drivers for the implementation of ISM strategy at KenGen. Key among these are: Business continuity where through ISM strategy organizational competencies were developed and preserved for the better performance of the Company. Information Security Management(ISM) needed to be part of the organization strategy in protecting company information, reports and general information. The need to protect information to support business and strategy. Information Commercial purpose to competing organizations. ISM strategy implementation faced several challenges including: lack of user awareness as KenGen staff did not understand what information security was all about and their role concerning the same. Lack of priority on ISM among employees. Employees were less willing to adopt and practice ISM because they felt comfortable in their then situations prior to the introduction of ISM strategy. The study further concludes that Several Strategies were adopted by KenGen to overcome the Challenges faced during implementation of ISM. The Company adopted a user awareness strategy using top down approach. There was better planning and restructuring in the organization where ISM function was moved to the right place in the organization. This study recommends that a thorough evaluation be conducted to establish the extent to which each of the drivers has been met. This study also recommends that the Company incorporates all staff in strategy formulation as the formulation of ISM strategies seems to have excluded some employees leading to greater resistance during implementation. The study further recommends that employees be trained on the importance of ISM strategy and how it affects the competitiveness of the Company. This will promote the level of adherence and observation of the policy.

TABLE OF CONTENTS

CHAPTER ONE

INTRODUCTION

1.1 Background of study

Information is a key resource for all enterprises and, from the time information is created to the moment it is destroyed, technology plays a significant role. Technology is increasingly advanced and has become pervasive in enterprises and the social, public and business environments (Johnston et al., 2008). Information is one of the most important enterprise assets. For any organization, information is valuable and should be appropriately protected (BSI, 1999).

The value of information goes beyond the written words and numbers: knowledge, concepts, ideas and brands are examples of intangible forms of information. Information and related processes, systems, networks and personnel involved in their operation, handling and protection are assets that, like other important business assets, are valuable to an organization's business. Information security is achieved by implementing a suitable set of controls, including policies, processes, procedures, organizational structures, software and hardware functions. These controls need to be established, implemented, monitored, reviewed and improved, where necessary to ensure that the specific security and business objectives of the organization are met (BSI, 1999).

Security is about managing risk, and risk management covers opportunity and threat. Consequently, the information security value proposition has two components:-business enablement and asset protection. Security covers people and process issues as well as technology, so security needs to be integrated into the enterprise risk management framework and cover the entire enterprise.

1.1.1 Concept of strategy

Ansoff and McDonnell (1990), describe strategy as asset of decision making rules for guidance of organizational behavior. Campbell et al., (2002) defined strategy simply as a vehicle through which a business can review past performance and, more importantly, determine future actions geared towards achieving and sustaining superior performance. Strategic management is therefore a vital tool in all organizations today as it helps business managers in making strategic decisions that affect the long term objectives of the organizations.

Ansoff (1998) argues that strategy assists companies to cope with change, which is usually precipated by environmental factors. Porter (1980) advances the view that strategy acts as the link between the firm and its environment. Thompson and Strickland (1998) are of the view that a good strategy needs to be ‘well matched’ to the external environment. As changes evolve in the environment, so must the strategy. Internally, strategy entails formulation and implementation of capabilities and resource strengths that are needed to sustain a competitive edge by the company. As a consequence of this, scanning the operating environment is crucial in order to detect new trends of paradigms, which may call for a change of strategy. Such developments could be in the economic, demographic, social, political or technological fields. The essence of strategy is to relate the organization to changes in the environment (Ansoff, 1987). Strategy therefore is a tool that helps the organization to align its activities to match turbulence in the environment. Organizations therefore need to develop response mechanisms to deal with the changes in the environment.

An Information Security Management (ISM) strategy provides an organization with a road map for information and information infrastructure protection with goals and objectives that ensure capabilities provided are aligned to business goals and the organization's risk profile (Mead and Stehney, 2005). Traditionally, ISM has been treated as an IT function and included in an organization's IT strategic planning. As ISM has evolved into a more critical element of business support activities, it now requires its own independent strategy to ensure its ability to appropriately support business goals and to mature and evolve effectively. Along with a security strategy and an associated security policy, the business must clearly define roles and responsibilities. Successful security strategy delivery incorporates clarity regarding business ownership and technology support responsibilities, as well as their interaction.

The key drivers towards information security strategy formulation and implementation include strategic alignment as discussed by Peltier (2013) in his study, who concluded that when strategically aligned, security functions as a business enabler that adds value. Risk management and regulatory compliance are among the drivers of ISM strategy implementation since it involves executing appropriate measures to manage risks and potential impacts to an acceptable level and many organizations find that they are subject to more than one set of regulations respectively (McNurlin, 1989; Stulz 1996).These drivers are important as they will dictate the ability of the organization to execute the strategy that has been defined.

1.1.2 Information Security Strategy Implementation

Strategy implementation is a process by which strategies and policies are put into action through the development of programs, budgets and procedures. Thompson and Strickland (1989) define it as the methods by which strategies are operationalized or executed within the organization; it focuses on the processes through which strategies are achieved. Strategy implementation includes the full range of managerial activities associated with putting the chosen strategy into place, supervising its pursuits and achieving the targeted results.

According to Kaplan and Norton (2001), business awareness is a key driver in the development of any strategy; this forms the first phase in ISM strategy development. When developing an ISM strategy, it is important to understand the organization's current business conditions, as they will dictate the ability of the organization to execute the strategy that has been defined. If an organization does not have the staff, budget or interest in a robust or expansive ISM capability, the strategy must reflect this situation. In many cases, organizations will implement effective capabilities only if those capabilities will reduce their capital and operational expenses or increase their value in the marketplace.

One of the vital and often misunderstood data points that must be considered when developing an ISM strategy is the organization's risk profile and appetite. The goal of an ISM strategy should be to complement business goals while maintaining a responsible level of risk management and security for the organization's information infrastructure and data. ISM is one component of an overall enterprise risk management (ERM) capability, and as such, it should align itself with the goals and doctrines of ERM whenever possible (Clarke and Varma, 1999).

The implementation phase and operation includes taking global considerations into account. Determining how compliant the organization wants or needs to be. Determine consequences of not conforming to ISM policies and requirements. Utilize an oversight board as part of the operational model for an ISM strategy. Ensure that appropriate communication is occurring between the ISM groups and supporting business (BSI, 1999).Some of the challenges highlighted in previous studies as concerns ISM strategy implementation include lack of awareness by staff members, lack of top management support and resources among others. Responsibility for security must be embedded into the culture of the organization from induction to exit, and must be resilient, changing as requirements change. Security awareness and responsibility must apply to those with external or temporary access rights to information assets, as well as permanent staff (Nnolim and Steenkamp, 2008).

1.1.3 The power Industry in Kenya

The Kenya Electricity Generating Company (KenGen) is one of the five power generating companies supplying electricity to the Kenya Power and lighting Company Ltd. (KPLC) in Kenya. From around mid-1997, power generation has been liberalized and hence we have a mix of both public and private entities in the sector. For many years, KenGen was considered a monopoly in Kenya in that it was the only organization responsible for producing electricity. The environmental turbulence has posed various challenges such as increased competition, high cost of power production and international pressure on conservation of the environment for the benefit of the whole world. This has led to the licensing of other firms to produce power and these firms are referred to as Independent Power Producers (IPP’s). KenGen still dominates the power production market in Kenya with 77% of the sales. However the IPP's are slowly eating into KenGen's market share as their number increases and also their capacity increases.

All the power production and transmission companies are regulated by the government's ministry of energy through the Energy Regulatory Commission (ERC). ERC was established as an Energy Sector Regulator under the Energy Act, 2006 in July 2007. ERC is a single sector regulatory agency, with responsibility for economic and technical regulation of electric power, renewable energy, and downstream petroleum sub-sectors, including tariff setting and review.

1.1.4 Kenya Electricity Generating Company (KenGen)

The Kenya Electricity Generating Company, KenGen, has a history that dates back to 1954. In this year, The Kenya Power Company (KPC) was registered as a company and commissioned to construct the transmission line between Nairobi and Tororo in Uganda as well as to develop geothermal and other generating facilities in the country. Since its inception, the Kenya Power and Lighting Company (KPLC), to which it sold electricity in bulk at cost, managed the company, under a management contract. In January 1997, the management of KPC was formally separated from KPLC as a direct result of the new reforms being undertaken in the energy sector and the entire economy.

On October 2nd 1998, KPC was re-launched under a new name and corporate identity, The Kenya Electricity Generating Company Ltd. - KenGen was born. KenGen, at its launch hence took charge of all publicly owned power generating plants.KenGen is a limited liability company registered under the Company's Act and 70% owned by the Government of Kenya and 30% publicly owned. Its core Activity is electric power generation (KenGen Annual Report, 2003). Kenya Electricity Generating Company Limited, KenGen is the leading electric power generation company in Kenya, producing about 80 percent of electricity consumed in the country. The company utilizes various sources to generate electricity ranging from hydro, geothermal, thermal and wind. KenGen has a workforce of over 1,500 staff located at different power plants in the country. With its wealth of experience, established corporate base and a clear vision, the company intends to maintain leadership in the liberalized electric energy sub-sector in Kenya and the Eastern Africa Region.

1.2 Research problem

Once strategies have been developed, they need to be implemented; they are of no value unless they are effectively translated into action (Aosa, 1992). Mintzberg and Quinn (1991) stated that 90% of well formulated strategies fail at implementation stage while only 10% of formulated strategies are successfully implemented. An information security management (ISM) strategy provides an organization with a road map for information and information infrastructure protection with goals and objectives that ensure capabilities provided are aligned to business goals and the organization's risk profile. As ISM has evolved into a more critical element of business support activities, it now requires its own independent strategy to ensure its ability to appropriately support business goals and to mature and evolve effectively (Peltier, 2013).

KenGen, like many other organizations, is constantly faced with the challenges of adapting to changes in environmental conditions. For such organizations to survive, it is important to formulate and implement strategies that will counter such turbulence. According to Huczynski and Buchanan (2007), organizational change is a strategic imperative. This means that radical shifts or strategic change are required in order to cope with the many and unpredictable changes in the wider social, economic, political and technological environment. Such strategies may include benchmarking, information technology, ISMS, etc

Identifying, analyzing and understanding drivers of information security management enable organizations to implement the right practices and strategies to achieve a competitive organization. Without an idea of drivers, it becomes difficult to develop a clear information security strategy to deal with complexity. However, from the previous studies, a gap exists for empirical evidence on the information security strategy implementation drivers and the challenges. Although there are studies in Kenya for example Isaiah (2011) and Karuri (2006) dealing with strategy implementation, Muratha (2012) dealing with information security, none of them has addressed the challenges faced during Information Security management strategy implementation in KenGen (Luftman, 2004; Dhillon & Backhouse, 2000; Stulz, 1996). In addition, since there has not been a prior research on the challenges inhibiting successful implementation of ISM strategy in KenGen, this research was worth undertaking. What are the drivers and challenges towards implementation of ISMS in KenGen?

1.3 Research objectives

The objectives of this study were:

i. To establish drivers of the information security strategy implementation in KenGen.

ii. To establish the challenges in information security strategy implementation in KenGen.

1.4 Value of the Study

This study sought to establish the challenges facing the implementation of the information security management strategy in KenGen. Taking into account the organization's overall business strategy and objectives. Through this study, the author formulated a foundation of a research program which sought to address the various facets of the implementation of an information security management strategy in an organization. How it correlates to the main business strategy and objectives and significant challenges faced by KenGen in the process formulation, implementation and maintenance of the strategy.

The report of this study would be an important source of information to stakeholders, members of the society and other parties who have a stake in the welfare of KenGen. It would also be a valuable platform for managers in trying to understand information security as well as the challenges in ISM strategy formulation and implementation and how to address them. The report would also provide suggestions to other organizations in the power industry on how to improve on professional practices in ISM strategy implementation. KenGen being a state corporation, this report would be useful to the policy makers in making decisions on the management of the company.

CHAPTER TWO

LITERATURE REVIEW

2.1 Introduction

Literature review is very important in research because it sharpens and deepens the theoretical foundation of the research (Kombo and Tromp, 2006). It enables the researcher to study other similar researches that have been undertaken in areas similar to the area of study. This facilitates insight development into what has been done by other researchers, with which the researcher is able to formulate an appropriate research and address research gaps.

This chapter focuses on the review of the literature on information security strategy. The main areas covered are, information security strategy formulation and implementation, drivers for the ISM implementation and the challenges as well. It also covers the theoretical framework and conceptual framework.

2.2 Theoretical basis of Study

A theoretical framework provides a rationale for predictions about the relationships among variables of a research study and has implications for every decision made in the research process (Mertens, 1999). The study is founded on three theories:-the management information theory, contingency theory and integrated systems theory. Management system theory emphasizes that an organization should establish and maintain a documented information security management system (ISMS) to control and protect information assets.

Contingency theory emphasizes that information security management is a part of contingency management that is meant for the prevention, detection and reaction to the threats, vulnerabilities and impacts inside and outside of an organization. The integrated systems theory is based on contingency management and integrates information security policy, risk management, internal control and information auditing theories to form an Information Security Architecture that is consistent with organizational objectives.

2.2.1 Management system theory

Management systems theory looks at the relationships between the organizations and the environment in which they are involved. This focus reflects on organizations' ability to adapt to changes in environmental conditions (Boulding, 1956; Katz and Kahn, 1978). Based on the organizational requirements and security strategies, Sherwood (1996) proposed information security architecture SALSA (Sherwood Associated Limited Security Architecture) which includes: business requirements, major security strategies, security services, security mechanism; and security products and technologies.

This theory informs the study since it emphasizes that an organization should establish and maintain a documented information security management system (ISMS) to control and protect information assets. ISMS include six steps: define the policy, define the scope of ISMS, undertake a risk assessment, manage the risk, select control objectives and control to be implemented; and prepare a statement of applicability (BSI, 1999). Organizations should inspect the environments and security standards to establish an information security policy, define the scope of information security and assess the risk and control in order to form an information security management system.

2.2.2 Contingency theory

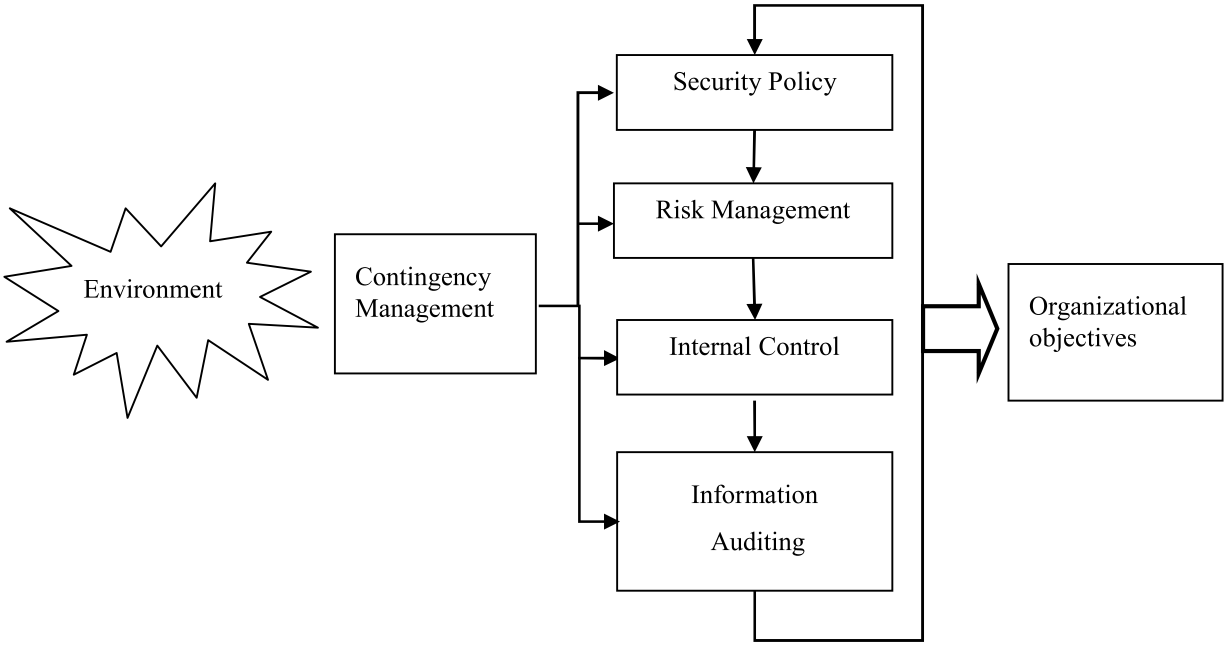
Contingency theory states that there is no one best way to structure and manage organizations. According to their research based on management of innovation, Burns and Stalker (1968), found out that organizational systems should vary based on the level of stability in the environment. Contingency approach is to recognize and respond to situational variables in order to attain organizational objectives effectively (Drazin and VandeVen, 1985). Contingency management is to manage the interaction between a set of environmental variables and another set of technological and managerial variables, and the goal is to strive for the attainment of organizational objectives (Lee et al., 1982; Luthans, 1976). Therefore, to take on policy-oriented managerial activities or risk management activities is dependent upon an organization's contingency strategy.

This theory informs the study since contingency approach has been applied to information security management. For example, Solms et al. (1994) proposed an information security model (ISM) which consist of five information security levels: ideal; prescribed; baseline; current; and survival. Except for the ideal level, all the other four levels are dynamic and contingent upon environmental variables such as information security threats, vulnerabilities and impact for an organization. The procedures for coping with organizational information security problems are most undefined since the procedures are dependent upon several situational variables.

Therefore, to take on policy-oriented managerial activities or risk management activities is dependent upon an organization's contingency strategy.

2.2.3 An integrated systems theory

Fig 1: A dramatic illustration of integrated system theory



Source: (Hong, Chi, Chao, & Tang, 2003, p. 253-248)

According to Hong et al (2003), an integrated systems theory is based on contingency management. To meet the demands of fast-changing environment, any component of managerial activities could be the focus. They further argued that organizations nowadays rely heavily on information technology and information security has caught a great deal of attention; however, few information security strategies and guidelines could be found for practitioners. This may result from a lack of coherent and comprehensive information security management theory. This theory integrates different perspectives from security policy, risk management, control and auditing, management systems and contingency theories and builds an integrate System Theory, which may lay a more solid foundation for further empirical studies. This theory informs the study since it explains organizational behavior regarding information security management, and provides alternatives for organizational security management strategies (BS 7799-2, 1999). This could be applied to predict the organizational attitudes and behavior towards information security management, and could be beneficial for information security decision making (Solms, 2004).

2.3 Information Security strategy formulation and implementation

Studies have shown that information residing in an organization is, in most instances the single most critical asset .Government and commercial organizations rely heavily on the use of information to conduct their business activities. Compromise of confidentiality, integrity, availability, non-repudiation, accountability, authenticity and reliability of an organization's assets can have an adverse impact (Pearson et al, 2008).

According to Dhillon and Backhouse (2000), there is a critical need to protect information and to manage the security of Information and Communication Technologies (ICT) systems within organizations. This requirement to protect information is particularly important in today's environment because many organizations are internally and externally connected by networks of ICT systems not necessarily controlled by their organizations. As well, legislation in many countries requires that management take appropriate action to mitigate risk related to the business and the use of ICT systems. Such legislation may cover not only privacy/data protection but also healthcare and financial markets, among others.

In developing an information security strategy, business awareness is key, Kaplan and Norton (2001) and it forms the first phase which includes understanding of the organization’s current business conditions and the organization’s risk profile and appetite Clarke and Varma (1999). These factors are important as they will dictate the ability of the organization to execute the strategy that has been defined. If an organization does not have the staff, budget or interest in a robust or expansive ISM capability, the strategy must reflect this situation. In many cases, organizations will implement effective capabilities only if those capabilities will reduce their capital and operational expenses or increase their value in the market place.

Strategy definition follows which consists of a prescriptive annual plan followed by a rolling three-year plan. It clearly identifies the point of arrival for capabilities based on management guidance and input. Ensure the availability and capability of necessary staff for the strategy execution. Gain an understanding of the organization’s culture to ensure an appropriate plan for ISM strategy adoption (Pramod et al, 2013)

Strategy development is the third phase which defines the governance model and functional inventory of capabilities and services .It involves considering whether the ISM strategy will include operational components or will act as a consultative element within the organization (Hedley, 1996). Determining the reporting structure for ISM, considering the staff and competency requirements necessary to successfully implement and operate the ISM strategy Kaplan and Norton (2002). Consider the risks of sourcing and ensure appropriate oversight by internal staff. Metrics and benchmarking should ensure alignment with industry standards and guidelines. According to (Keyes, 2005), the use of a capability maturity model (CMM) assessment methodology was recommended. (Tsang, 1998) also proposed the use of KPIs to measure the effectiveness of the functions and capabilities developed through the ISM strategy.

The implementation phase and operation includes taking global considerations into account. (Porter, 1990) defined strategy implementation as the process of allocating resources to support the chosen strategies. This process includes the various management activities that are necessary to put strategy in motion, institute strategic controls that monitor progress, and ultimately achieve organizational goals. Compliance is currently the driving force behind many ISM strategy development activities. A better approach often is to analyze the impact of not being compliant or becoming only partially compliant. According to Kim and Malbougne (1993) if a regulation or standard does not have court precedence or defined and implemented consequence management, the impact of noncompliance may not be well understood. It may be in the organization's best interest to continue to develop capabilities in line with industry-leading and organizational best practices instead of focusing on external compliance requirements alone.

2.4 Drivers of ISM strategy implementation

Aligning security activities with business strategy to support organizational objectives as described by Luftman (2004) is one of the key drivers of ISRM strategy implementation. Its Alignment is to optimize the value that ISRM contributes to the enterprise. According to Chan, et al, (2001) an organization has successfully aligned ISRM strategy to business strategy when there is a shared understanding of how information, applications, technologies and services will contribute to business objectives – today and in the future. Also, a shared focus on where to expend scarce resources, time and money; the tradeoffs the enterprise is prepared to make and a credible working relationship between the IT organization and the rest of the business evidenced by reliable daily operations, responsive problem management and predictable, innovative solution delivery (Santana et al, 2008).

When strategically aligned, security functions as a business enabler that adds value (Peltier, 2013). Security is an expected topic of discussion among decision makers and is given the same level of respect as other fundamental drivers and influencing elements of the business. This requires leadership that recognizes the value of information security, invests in people and processes, encourages discussion and debate, and treats security in the same fashion as every other business requirement. Solms (2005) explains that information security professionals should recognize that the true value of information security is protecting the business from harm and achieving organizational objectives. Visible management support coupled with written policy formalizes and communicates the organizational commitment to information security.

According to Stulz (1996), risk management involves executing appropriate measures to manage risks and potential impacts to an acceptable level. Organizations use information systems to collaborate and share information. Innovative companies build value through new online processes and transactions, and the free exchange of ideas. At the same time, the information that increasingly makes up the bulk of the value of a company needs to be protected and business risks minimized. Ellemers (1993) proposed that strong identity management can help control who gains access to information and with what permissions.

Many organizations find that they are subject to more than one set of regulations. Organizations that try to write their policies to match federal state regulations find the task daunting. Fortunately, the regulations published to date have enough in common that a well-written set of information security policies based on a framework such as the ISO 27002 can be mapped to multiple regulatory requirements. Policy administrative notations will often include a cross-reference to specific regulatory requirements (McNurlin, 1989).

2.5 ISM Implementation Challenges

Strategies are critical elements in organizational functioning, but whereas many organizations have good strategies, successful strategy implementation remains a challenge. To ensure success the strategy must be translated into carefully implemented actions (Pearce and Robinson, 1997). Many organizations design excellent strategies but fail at implementation (Karuri, 2006).

Organizations should have a comprehensive ISMS plan and assign to specific people the exact areas that they should be responsible for protecting against security breaches. In reality, very few such plans are available, making it hard to gauge the plan's implementation success (Okumus, 2001). The inability for the personnel to segregate and dedicate their duties to perform the ISMS tasks on top of their daily job activities has contributed to the delay or failure to implement ISMS strategy properly.

Besides that, support from top management in most organizations falls below expectations (Lyles, 1992). This raises the question of commitment: has management grasped the size of the impact of a serious security violation on sensitive company information? An attack is a very real threat that can happen at any moment. If organizations are seriously concerned about data security, then the people at the top should involve themselves with their project teams' right from the start, scrutinizing their ideas, plans and budgets.

According to Macintos (1984), policies, procedures and guidelines which are not expertly scripted are another challenge. After all, the ISM strategy requires documenting every implementation phase as proof of completion and as a reference point for employees, auditors and other relevant parties. The majority of the organizations in the pilot program do not have sufficient/appropriate security policies, procedures and guidelines in place. Among the reasons is that because they do not have knowledgeable and experienced staff capable of writing appropriate policies and also because they did not manage to carry out the risk assessment process comprehensively and thus they were not able to come up with the appropriate policies, procedures & guidelines based on the risk assessment results. Muratha (2012) concluded that security is more than just a technological problem, she further identified that human aspect has not been given much attention hence most of the security breaches. She went ahead and highlighted that information security policies are backbone of any effective information security program. In a few other organizations though, such documentations already exist but the quality of writing leaves much to be desired.

In his studies, Kaplan and Norton (2004) identified inadequate asset listing as a key challenge. Comprehensive listing meticulously identifies assets most prone to security violations so that plans can be developed to mitigate risks occurring to them. It is essential for carrying out a thorough risk assessment. Clearly, organizations with a less well-endowed listing actually make themselves vulnerable to security attacks. Controls which are not competent enough to mitigate the identified risks efficiently are also another challenge. They could be if the people developing the controls are able to link them to the variety of sources from which risks may come. Then risk mitigation should become more efficient. Most organizations, surprisingly, have not fully assessed the impact that external and internal threats can have on data protection while some have not even defined an acceptable level of risks that they can take should a security breach occur (BSI, 1999).

Justifying the investment of a system is usually a challenge in many organizations and ISM is not an exception of the systems receiving such resistance. In addition, Pollard (2005) argues that the challenges faced today in getting people to share what they know and to collaborate effectively are not caused or cured by technologies, but are cultural impediments. He further argued that it is extremely difficult to change people's behaviors and so the solutions need to accommodate these behaviors, and these cultures, rather than trying to 'fix' them. Therefore, knowledge in itself without the right strategy for dissemination may not be of much value to an organization. As a result ignoring the organization culture can pose a challenge towards acceptance of ISRM strategy.

Finally, some of the participating organizations lack continual management reviews. It is a question of commitment (Kaplan & Norton, 1996). This is actually detrimental to the very idea of data protection itself. Participating organizations should understand that constant reviews can put them on the track to successful data protection implementation. However, such reviews are few and far between. It is also discovered that for some of the organizations that do conduct regular reviews, most of the time these review meetings are not attended by the right personnel.

CHAPTER THREE

RESEARCH METHODOLOGY

3.1 Introduction

This chapter presents stages and phases that were followed in completing the study. It involves a blueprint for the collection, measurement and analysis of data. Specifically the chapter covers research design, data collection and data analysis.

3.2 Research Design

The research was conducted through a case study. A case study is one of several ways of doing research whether it is social science related or even socially related. The study requires an in-depth investigation and hence it is only appropriate to use a case study. Rather than using samples and following a rigid protocol to examine limited number of variables, a case study method involved an in-depth, longitudinal examination of a single instance or event and hence providing a systematic way of looking at events, collecting data, analyzing information, and reporting the results. As a result the researcher gained a sharpened understanding of why the instance happened as it did, and what might become important to look at more extensively in future research.

The aim is to equip the researcher with in-depth information on what challenges, KENGEN as an organization is facing in the implementation of ISM strategy and what drivers contributed to this implementation as far as information security is concerned. The case study is an appropriate research design as it undertakes in-depth analysis of KENGEN as a unit hence facilitates intensive study of the same.

3.3 Data Collection

Primary data was collected for the study. The primary data was gathered using the interview method. The focus was on top management who are the key people involved in strategic decisions. In this particular case, the five people to be interviewed included the Information and Communications Technology Manager, the Internal Audit & Risk Manager, the Legal Manager, the Human Resources manager and the Operations Manager.

Section one comprised general information, while section two aims to establish the drivers of ISM implementation. Section three of the interview guide aims to capture data on likely sources of implementation challenges of ISM strategy while section four looked at the strategies that if put in place, they countered these challenges.

3.4 Data Analysis

Data analysis is a practice in which raw data is ordered and organized so that useful information can be extracted from it. The process of organizing and thinking about data is key to understanding what the data does and does not contain. Summarizing data is often critical to supporting arguments made with that data, as is presenting the data in a clear and understandable way.

The content analysis technique was used to analyze the data. The findings emerging from the analysis were used to compile this report. Content analysis is defined as a technique for making inferences by systematically and objectively identifying specified characteristics of messages and using the same approach to related trends

(Nachmias and Nachmias, 1996). The qualitative method can be used to uncover and understand what lies behind the phenomena under study (Nyororo, 2006).

CHAPTER FOUR

DATA ANALYSIS, RESULTS AND DISCUSSION

4.1 Introduction

This chapter presents and discusses the analysis of the data collected from the various respondents. The data was also analyzed using the procedures indicated in chapter three above. The data analyzed in this chapter is based on the interview guide questions which were presented to the respondents by the researcher. The data is presented in prose according to the thematic areas covered in the interview guide.

4.2 General information

The study sought to collect some background information about the respondents that were interviewed. The interviewees were requested to indicate their position at Kenya Electricity Generating Company (KenGen). From the responses, the interviewees worked in various departments. These included the Information and Communications Technology, the Internal Audit & Risk, Legal, Human Resources and operations. These ensured that the data collected was representative of the organization as the almost all the departments were included in the study.

The study further sought to establish the period that the respondents had worked with KenGen. From the responses, it was established that the interviewees had worked with the company for between thirteen to 25 years. This demonstrated their level of understanding of the operations in the Company hence was better placed to provide responses for the study. In addition, the study sought to establish the period that the interviewees had served in their current positions. From the findings, the interviewees had served in the current position for at least four years while long serving interviewees had served for 16 years. These findings show that the respondents had served in their current positions long enough to understand the drivers and challenges of the information security strategy implementation in KenGen.

Another general question inquired from the interviewees as to whether they had heard of Information Security management strategy at KenGen. From the responses, all the interviewees indicated that they had heard of Information Security management strategy at KenGen and that if formed part of the key strategies especially geared towards protecting company secrets. On its meaning, the interviewees indicated that it entailed the controls and the need to know and who anyone in the Company is sharing the company information with. It cuts across the organization and it is not an information technology function. Other respondents understood it to mean information security involving both the IT side and cut across the whole organization at large. They generally indicated that it was meant for providing direction on the way to secure information. The other meaning included it being an IT function which dealt with protection ICT systems to prevent unauthorized access to the same. From these findings, it is clear that the respondents held various meanings for Information Security management strategy. However, they generally had a clue on what it meant though not very precisely.

4.3 Drivers for implementation of ISM strategy in KenGen

The interviewees were requested to identify some of the driving forces towards implementation of Information Security Management strategy at KenGen. From the responses, the interviewees identified a number of drivers. These included Business continuity where the interviewees indicated that through ISM strategy organizational competencies were developed and preserved for the better performance of the Company. The interviewees also indicated that ISM availed a system to prevent compromised or unauthorized access to company information thereby protecting company secrets. The interviewees also indicated that ISM was important for strategic alignment of the organization to the operating environment. The interviewees noted that ISM should be part of the organization strategy in protecting company information, reports and general information.

The interviewees noted that another driver for ISM strategy was to enable compliance with the regulatory requirements and especially the organization's ISO 27002-information security implementation standards. This standard requires the Company to protect its information system and ensure that information does not get into the wrong hands. Another driver for the implementation of ISM strategy included the need to protect information to support business and strategy. For instance, in the geothermal, the information is enormous and it can be used to support or derail the business strategy.

Another driver for the implementation of ISM strategy at KenGen included information commercial purpose to competing organizations. The ISM KenGen was able to collect and store information relevant on the market forces including customer demands and views. The Company was then able to utilize this information to improve service delivery to customers. The interviewees also noted that ISM enabled KenGen make timely and quality decisions as information is about decisions and it is powerful. The Company used this information to create user awareness, create a learning organization and protect huge data, for instance data concerning wind from leakage or unauthorized access to competitor's i.e independent power producers.

The interviewees noted a case of the Menengai land which was grabbed from KenGen due to information leakage on the plans which were underway. The interviewees also noted a case where KenGen lost a lot of data to Geothermal Development Company (GDC) when it was formed due to leakage and lack of information security measures. Other drivers of ISM implementation are to manage organization risk, business continuity, and strategic alignment. The implementation of ISM has enabled the Company to only have the right personnel handling projections on the right information thus maintaining its competitive edge over independent power producers. In addition, the interviewees noted that the scientific investigations in geothermal area which are ongoing drives the need for protection of information from the competitors hence ISM implementation. They illustrated how important ISM was in management of secrets in the Company for competitive advantage.

4.4 Challenges Facing Implementation of ISM Strategy Implementation

The interviewees were requested to identify the challenges that KenGen faced in the implementation of information security strategy. The interviewees identified a number of challenges including lack of user awareness as KenGen staff did not understand what information security was all about and their role concerning the same. As a result, they did not clearly understand how, when and where to share certain information and with whom. This led to leakage of company secrets which brought about huge losses like in the case where KenGen lost a lot of data to Geothermal Development Company when it was formed due to leakage and lack of information security measures.

Another challenge noted by the interviewees included limited priority on ISM among employees. They indicated that ISM was not given priority even within IT department as indicated by poor allocation of resources on the same. In addition, senior managers were not aware of what ISM entails hence offered less support on the same. In addition, the culture in the organization was found to be a big challenge. Being a parastatal, most employees did not give their full potential in their duties. The interviewees indicated that some departments worked as though they were in competition instead of working together as a team. This reduced synergies hence negatively affecting ISM implementation.

Another challenge noted by the interviewees included resistance among employees to adhere to the provisions of ISM strategy guidelines. The employees were less willing to adopt and practice ISM because they felt comfortable in their then situations prior to the introduction of ISM strategy. This was largely because employees did not have adequate knowledge on the risks involved and losses which can be incurred in case of sabotage resulting from leaked information. The interviewees indicated that the ISM strategy had not been well communicated to staff hence not all staff were aware of it. Therefore its implementation faced a lot of resistance among other challenges.

The interviewees also noted that KenGen lacked adequately skilled experts on matters information security. The people appointed to oversee the ISM strategy implementation did not have adequate skills on information security matters but they learned on the job hence could not predict some scenarios and develop stop gap measures in time. The interviewees also noted that there was a challenge in the organization structure where ISM was placed under Information Communications Technologies department instead of creating a under security and integrity manager docket for this purpose. This therefore meant that the ISM was not given its due importance. There was limited senior staff spearheading information security matters hence limited management support. This led to limited support during the implementation stage. In addition, the interviewees noted that there was lack of responsibility and accountability on who controls what goes out there. Information is not arranged in any particular order but it is upon the user with rights to access and determine what to do with it in decision making. There was also limited user awareness on information importance as there was no clear strategy on ISM.

The interviewees indicated that these challenges greatly affected the information security management strategy implementation at KenGen. These challenges influenced the level of acceptance among staff to adopt the ISM strategy. Since the senior management was less involved in the strategy, this reduced the speed of implementation and the accuracy levels.

4.5 Strategies to overcome the Challenges faced during implementation of ISM

The interviewees were requested to indicate the strategies adopted by KenGen to overcome the Challenges faced during implementation of ISM. Several strategies were identified by the interviewees as having been adopted to overcome the identified challenges. First, the Company organized a create the need forum and made presentations on where the idea can be sold. This involved all employees and was organized first at the departmental level before being consolidated. This ensured that each and every employee understood the purpose of the strategy and what it meant to protect company information.

This also helped reduce the level of employee resistance hence promote implementation and adherence to the set ISM strategy.

The interviewees also noted that the Company adopted a user awareness strategy using top down approach. This started from the top management where need for ISM strategy was communicated and urged to support the strategy implementation. This involved appointment of some of the senior managers in the Company to champion the implementation. These managers acted as change implementation agents. This improved the level of senior management support and the overall implementation of the strategy. This also promoted the level of ownership of the strategy among senior management.

The interviewees further noted that there was better planning and restructuring in the organization where ISM function was moved to the right place in the organization. It was made an autonomous department reporting direct to the Chief Executive Officer and the Board. This promoted the level of monitoring on the implementation as now there was clear demarcation of what the team needed to do.

The interviewees further noted that the organization organized training sessions on ISM to empower staff on the importance of information system management strategy. This increased the level of appreciation among staff of the ISM strategy. As a result, it reduced the level of employee resistance. The organization also developed clear ISM policies and procedures so that every action was well guided and information retrieval was easy. This also involved clear documentation of what the information requested by any given staff was meant for and on a daily basis, a record of the information accessed by each staff was kept. This promoted the level of consciousness among staff when dealing with company information.

4.6 Discussion of the findings

The study revealed that ISM strategy organizational competencies were developed and preserved for the better performance of the Company. This is in line with the work of Luftman (2004) who posited that aligning organizational activities with business strategy to support organizational objectives is one of the key drivers of ISRM strategy implementation. The interviewees also indicated that ISM availed a system to prevent compromised or unauthorized access to company information thereby protecting company secrets. The study also revealed that ISM was important for strategic alignment of the organization to the operating environment. The interviewees noted that ISM should be part of the organization strategy in protecting company information, reports and general information. ISM availed a system to prevent compromised or unauthorized access to company information thereby protecting company secrets. These findings are consistent with the argument of Luftman (2004) that aligning security activities with business strategy to support organizational objectives is one of the key drivers of ISRM strategy implementation.

Another driver for the implementation of ISM strategy included the need to protect information to support business and strategy. Another driver for the implementation of ISM strategy at KenGen included information Commercial purpose to competing organizations. When strategically aligned, security functions as a business enabler that adds value (Peltier, 2013).

The process of ISM strategy implementation came with a number of challenges. Some of these included: lack of user awareness as KenGen staff did not understand what information security was all about and their role concerning the same. Employees did not clearly understand how, when and where to share certain information and with whom. To ensure success the strategy must be translated into carefully implemented actions (Pearce and Robinson, 1997). Many organizations design excellent strategies but fail at implementation (Karuri, 2006). The inability for the personnel to segregate and dedicate their duties to perform the ISMS tasks on top of their daily job activities has contributed to the delay or failure to implement ISMS strategy properly. Muratha (2012) concluded that security is more than just a technological problem, she further identified that human aspect has not been given much attention hence most of the security breaches. There was also lack of priority on ISM among employees. ISM was not given priority even within IT department as indicated by poor allocation of resources on the same. In addition, senior managers were not aware of what ISM entails hence offered less support on the same.

The culture in the organization was found to be a big challenge. Being a parastatal, most employees did not give their full potential in their duties. Resistance among employees to adhere to the provisions of ISM strategy guidelines. The employees were less willing to adopt and practice ISM because they felt comfortable in their then situations prior to the introduction of ISM strategy. There was limited senior staff spearheading information security matters hence limited management support. This led to limited support during the implementation stage. Information was not arranged in any particular order but it is upon the user with rights to access and determine what to do with it in decision making. Kaplan and Norton (2004) identified inadequate asset listing as a key challenge. Comprehensive listing meticulously identifies assets most prone to security violations so that plans can be developed to mitigate risks occurring to them. It is essential for carrying out a thorough risk assessment.

Several Strategies were adopted by KenGen to overcome the Challenges faced during implementation of ISM. These included: the Company organized a create the need forum and made presentations on where the idea can be sold. The Company adopted a user awareness strategy using top down approach (Kaplan & Norton, 1996). This started from the top management where need for ISM strategy was communicated and urged to support the strategy implementation. There was better planning and restructuring in the organization where ISM function was moved to the right place in the organization. It was made an autonomous department reporting direct to the Chief Executive Officer and the Board. The organization organized training sessions on ISM to empower staff on the importance of information system management strategy. This is actually detrimental to the very idea of data protection itself. Participating organizations should understand that constant reviews can put them on the track to successful data protection implementation (BSI, 1999).

CHAPTER FIVE

SUMMARY, CONCLUSIONS AND RECOMMENDATIONS

5.1 Introduction

This chapter discusses the findings of the research and draws conclusions from the major findings. The study was on information security management strategy implementation challenges at Kenya Electricity Generating Company. This chapter seeks to bring out the main findings of the research and offer recommendation based on the results of the study.

5.2 Summary of the Findings

Several drivers were identified for implementation of ISM strategy at KenGen. These included Business continuity where through ISM strategy organizational competencies were developed and preserved for the better performance of the Company. ISM availed a system to prevent compromised or unauthorized access to company information thereby protecting company secrets. ISM was important for strategic alignment of the organization to the operating environment. ISM needed to be part of the organization strategy in protecting company information, reports and general information. Another driver for Ism strategy was to enable compliance with the regulatory requirements and especially the organization's ISO 27002-information security implementation standards. Another driver for the implementation of ISM strategy included the need to protect information to support business and strategy. Another driver for the implementation of ISM strategy at KenGen included information Commercial purpose to competing organizations. The ISM KenGen was able to collect and store information relevant on the market forces including customer demands and views. ISM enabled KenGen make timely and quality decisions as information is about decisions and it is powerful. The implementation of ISM has enabled the Company to only have the right personnel handling projections on the right information thus maintaining its competitive edge over independent power producers. The scientific investigations in geothermal area which are ongoing drives the need for protection of information from the competitors hence ISM implementation.

However, the process of ISM strategy implementation came with a number of challenges. Some of these identified by the interviewees included; lack of user awareness as KenGen staff did not understand what information security was all about and their role concerning the same. Employees did not clearly understand how, when and where to share certain information and with whom. There was also lack of priority on ISM among employees. ISM was not given priority even within IT department as indicated by poor allocation of resources on the same. In addition, senior managers were not aware of what ISM entails hence offered less support on the same. The culture in the organization was found to be a big challenge. Being a parastatal, most employees did not give their full potential in their duties. Resistance among employees to adhere to the provisions of ISM strategy guidelines. The employees were less willing to adopt and practice ISM because they felt comfortable in their then situations prior to the introduction of ISM strategy. The ISM strategy had not been well communicated to staff hence not all staff were aware of it. KenGen lacked adequately skilled experts on matters information security. The people appointed to oversee the ISM strategy implementation did not have adequate skills on information security matters but they learned on the job hence could not predict some scenarios and develop stop gap measures in time. There was limited senior staff spearheading information security matters hence limited management support. This led to limited support during the implementation stage. Information was not arranged in any particular order but it is upon the user with rights to access and determine what to do with it in decision making. There was also limited user awareness on information importance as there was no clear strategy on ISM.

Several Strategies were adopted by KenGen to overcome the Challenges faced during implementation of ISM. These included: the Company organized a create the need forum and made presentations on where the idea can be sold. These involved all employees and were organized first at the departmental level before being consolidated. The Company adopted a user awareness strategy using top down approach. This started from the top management where need for ISM strategy was communicated and urged to support the strategy implementation. There was better planning and restructuring in the organization where ISM function was moved to the right place in the organization. It was made an autonomous department reporting direct to the Chief Executive Officer and the Board. The organization organized training sessions on ISM to empower staff on the importance of information system management strategy. This increased the level of appreciation among staff of the ISM strategy. As a result, it reduced the level of employee resistance. The organization also developed clear ISM policies and procedures so that every action was well guided and information retrieval was easy.

5.3 Conclusion

From the findings in chapter four and the summary of findings above, the study concludes that there were several drivers for the implementation of ISM strategy at KenGen. Key among these are: Business continuity where through ISM strategy organizational competencies were developed and preserved for the better performance of the Company. ISM was important for strategic alignment of the organization to the operating environment. ISM needed to be part of the organization strategy in protecting company information, reports and general information. Ism strategy was to enable compliance with the regulatory requirements and especially the organization's ISO 27002-information security implementation standards. The need to protect information to support business and strategy. Another driver for the implementation of ISM strategy at KenGen included information Commercial purpose to competing organizations. ISM enabled KenGen make timely and quality decisions as information is about decisions and it is powerful. The implementation of ISM has enabled the Company to only have the right personnel handling projections on the right information thus maintaining its competitive edge over independent power producers.

ISM strategy implementation faced several challenges including: lack of user awareness as KenGen staff did not understand what information security was all about and their role concerning the same. Lack of priority on ISM among employees. ISM was not given priority even within IT department as indicated by poor allocation of resources on the same. Senior managers were not aware of what ISM entails hence offered less support on the same. Employees were less willing to adopt and practice ISM because they felt comfortable in their then situations prior to the introduction of ISM strategy. The strategy had not been well communicated to staff hence not all staff were aware of it. The people appointed to oversee the ISM strategy implementation did not have adequate skills on information security matters but they learned on the job hence could not predict some scenarios and develop stop gap measures in time. Information was not arranged in any particular order but it is upon the user with rights to access and determine what to do with it in decision making.

The study further concludes that Several Strategies were adopted by KenGen to overcome the Challenges faced during implementation of ISM. The Company organized a create the need forum and made presentations on where the idea can be sold. The Company adopted a user awareness strategy using top down approach. There was better planning and restructuring in the organization where ISM function was moved to the right place in the organization. The organization organized training sessions on ISM to empower staff on the importance of information system management strategy. The organization also developed clear ISM policies and procedures so that every action was well guided and information retrieval was easy.

5.4 Recommendations

The findings of the study indicate that there were several drivers for the implementation of ISM strategy at KenGen. This study recommends that a thorough evaluation be conducted to establish the extent to which each of the drivers has been met. The implementation of all strategies is guided by set goals. This study therefore recommends that an evaluation be conducted to establish how the organization is performing on the set goals so as to know how to re-strategies to ensure that the Ism strategy goals are not missed.

This study also recommends that the Company incorporates all staff in strategy formulation as the formulation of ISM strategies seems to have excluded some employees leading to greater resistance during implementation. The study further recommends that employees be trained on the importance of ISM strategy and how it affects the competitiveness of the Company. This will promote the level of adherence and observation of the policy.

5.5 Limitations of the Study

A limitation for the purpose of this study was considered as any condition that affected the achievement of the study objectives. Some of these limitations included difficult to collect all data given the short time the interviewees set for the interviews. The target respondents for this study were busy managers with strict schedule hence making it difficult to have an elaborate interview session. To overcome this limitation, the researcher arranged for telephone interviews after the working hours to follow up on what had not been well explained.

In some instances, the meeting had to be rescheduled owing to the tight schedules that some managers operated and some never had time for the interviews. Another limitation for the study included the confidentiality nature of the information sought. Given the nature of Company's operations, the target managers were not quite comfortable with revealing all information during the interview.

5.6 Suggestions for Further Research

This study concentrated on information security management strategy implementation challenges at Kenya Electricity Generating Company. This was a case study of one autonomous government organization charged with the generation of electricity. This study therefore recommends that future studies be conducted on other organizations be it within Government institutions so as to allow for generalization of the findings.

The study further recommends that further studies be conducted to establish the effect of ISM on the competitiveness of organizations. The study needs to look at the benefits of knowledge management as a whole and how it influences organizational performance

REFERENCES

Ansoff, H. I. (1998). *Turbulence concept: Strategic management for difficult times*. Chichester: John Wiley

Ansoff, I., & McDonnell, E. (1990). *Implanting Strategic Management:* Prentice Hall, UK.

Aosa E. (1992), *An Empirical Investigation of Strategy Formulation and Implementation within Large Private Manufacturing Companies in Kenya,* Unpublished PHD Thesis, University of Strathclyde, Scotland, Feb.

Boulding, K. (1956). *General Systems Theory - The Skeleton of Science.* Management Science. 2(3), 197-208, reprinted in General Systems, Yearbook of the Society for General Systems Research, 1.

BSI, B. (1999). 7799-2: 1999, *Information Security Management Part 2: Specification for Information Security Management Systems*. British Security Institute*: UK*.

Campbell, D., Stonehouse, G., & Houston, B. (2002). *Business Strategy, an Introduction, 2nd Edition,* Butterworth – Heinemann, Great Britain.

Clarke, C. J., & Varma, S. (1999). Strategic risk management: the new competitive edge. *Long Range Planning*, *32*(4), 414-424.

Daft, R. L., & Macintosh, N. B. (1984). The nature and use of formal control systems for management control and strategy implementation. *Journal of Management*, *10*(1), 43-66.

Dhillon, G., & Backhouse, J. (2000). *Technical opinion: Information system security management in the new millennium*. Communications of the ACM,*43*(7), 125-128.

Drazin, R., & VandeVen, A.H. (1985). Alternative forms of fit in contingency theory, *Administrative Science Quarterly*, Vol. 30 No. 4, pp. 514-39.

Ellemers, N. (1993). The influence of socio-structural variables on identity management strategies. *European review of social psychology*, *4*(1), 27-57.

Hedley, B. (1976). A fundamental approach to strategy development. *Long Range Planning*, *9*(6), 2-11.

Hong, K. S., Chi, Y. P., Chao, L. R., & Tang, J. H. (2003). An integrated system theory of information security management. *Information Management & Computer Security*, *11*(5), 243-248.

Huczynski, A., & Buchanan, D. (2007). Organization Behavior. *Prentice-Hall*.

Isaiah, A. (2011).*Challenges facing the government of southern sudan in strategy implementation,* Unpublished MBA project, University of Nairobi.

Karuri,T,W.(2006).*Challenges of strategy implementation in development of financial institutions*.A case of industrial and commercial development corporation(ICDC).

Kaplan, R. S., & Norton, D. P. (2001). The strategy-focused organization.*Strategy and Leadership*, *29*(3), 41-42.

Katz, D., & Kahn, R.L. (1978). *The Social Psychology of Organizations*, II ed. New York: Wiley

Keyes, J. (2005). *Implementing the IT balanced scorecard: Aligning IT with corporate strategy*. CRC Press.

Kim, W. C., & Mauborgne, R. A. (1993). Procedural justice, attitudes, and subsidiary top management compliance with multinationals' corporate strategic decisions. *Academy of management journal*, *36*(3), 502-526.

Kombo, D. K., & Tromp, D. L. (2006). Proposal and thesis writing: An introduction. *Nairobi: Paulines Publications Africa*.

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.

Luftman, J. (2004). Assessing business-IT alignment maturity. *Strategies for information technology governance*, *4*, 99.

Lyles, M. A., & Schwenk, C. R. (1992). Top management, strategy and organizational knowledge structures. *Journal of Management Studies*, *29*(2), 155-174.

Luthans, F. (1976). *Introduction to Management*:A Contingency Approach, McGraw-Hill, New York, NY.

Ma, Q., Johnston, A. C., & Pearson, J. M. (2008). Information security management objectives and practices: a parsimonious framework. *Information Management & Computer Security*, *16*(3), 251-270

Mead, N. R., & Stehney, T. (2005). *Security quality requirements engineering (SQUARE) methodology* (Vol. 30, No. 4, pp. 1-7). ACM.

Mertens, D. M. (1999). Inclusive evaluation: Implications of transformative theory for evaluation. *American Journal of Evaluation*, *20*(1), 1-14.

McNurlin, B. C., Sprague, R. H., & Bui, T. X. (1989). *Information systems management in practice*. Prentice-Hall International

Mintzeberg, H., & Quinn, J.B. (1991). *The Strategy Process*, London: Prentice Hall.

Muratha, K.R. (2012). *Information Security practices in the Kenyan Capital Market*,Unpublished MBA project,University of Nairobi.

Nnolim, A. L., & Steenkamp, A. L. (2008). An Architectural and Process Model Approach to Information Security Management. *Information Systems Education Journal*, *6*(31), 1-27.

Nyororo, C. (2006). *Strategic Change Management and Performance of National Social Security Fund (NSSF),* Unpublished MBA project, University of Nairobi.

Okumus, F. (2001). Towards a strategy implementation framework. *International Journal of Contemporary Hospitality Management*, *13*(7), 327-338

Pearce, J., & Robinson, R. (2007).*Strategic Management ,Formulation and control*,10th edition,McGraw Hill

Peltier, T. R. (2013). *Information security fundamentals*. CRC Press.

Porter, M. E., & Millar, V. E. (1985). *How information gives you competitive advantage*.

Pramod, D., Raman, R., & Bharathi, S. V. (2013). An aspect oriented process based approach to information risk management. *International Journal of Engineering and Technology*, *5*(3), 2262-2267.

Santana ,T. R. G., Daneva, M., Eck, P. A. T., & Wieringa, R. J. (2008). *Towards a business-IT alignment maturity model for collaborative networked organizations.*

Sabherwal, R., & Chan, Y. E. (2001). Alignment between business and IS strategies: a study of prospectors, analyzers, and defenders. *Information systems research*, *12*(1), 11-33.

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

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

Solms, V.B. (2005). Information Security governance: COBIT or ISO 17799 or both? *Computers & Security*, *24*(2), 99-104.

Stulz, R. M. (1996). Rethinking risk management. *Journal of applied corporate finance*, *9*(3), 8-25.

Thompson, A., & Strickland III, A. J. (1989). *Strategy formulation and implementation: tasks of the general manager* (4th edition). BPI,IRWIN,Boston.

Tsang, A. H. (1998). A strategic approach to managing maintenance performance. *Journal of Quality in Maintenance Engineering*, *4*(2), 87-94.

APPENDICES

Appendix I: Letter of Introduction

Dear Respondent,

RE: REQUEST FOR RESEARCH DATA:

I am a postgraduate student pursuing a Masters degree in Business Administration in the School of Business, University of Nairobi. As a requirement for the completion of my studies, I am conducting a research on the drivers and challenges of information security management strategy implementation at Kenya Electricity Generating Company (KenGen).

To successfully undertake the study your cooperation and timely feedback will be highly appreciated. Kindly note that the information collected will be used purely for academic purposes and will be treated with utmost confidence.

Yours sincerely,

Faith Syombua Katua

Appendix II: Interview guide

Section I: General Information

1. What is your position at Kenya Electricity Generating Company (KenGen)?
2. How long have you worked at KenGen?
3. For how long have you held your current position?
4. Have you heard of Information Security management strategy at KenGen?
5. What does it mean and what is it meant to do?

Section II: Drivers for implementation of ISM strategy

6. What are some of the driving forces towards implementation of Information Security Management strategy at KenGen?
7. In what ways do the identified drivers influence the implementation of Information Security Management strategy at KenGen?

Section III: Challenges facing implementation of ISM strategy implementation

8. Information security implementation strategy has faced several challenges at KenGen. Kindly identify some of these challenges.
9. To what extent has these challenges influenced the information security management strategy implementation at KenGen?

Section IV: Strategies to overcome the Challenges faced during implementation of ISM

10. In order to ensure successful implementation of information security management strategy, KenGen has developed several responses to the above challenges; kindly identify some of these response strategies.
11. To what extent have the response strategies been effective in promoting information security management implementation in KenGen?

Your time is highly valued. Thank you

Appendix III: Research gaps summary

Study	Type	Theory Applied	Focus & Findings of study	Gap
(Luftman)	Research Paper	Contingency theory	Assessing Business-IT alignment. Strategic alignment is the key to achieving a competitive organization.	The study by Luftman (2004) focused only on strategic alignment as the main driver for information security implementation, as a way of achieving a competitive organization. My research will broaden the study to focus on other drivers which contribute to successful ISM implementation like top management involvement, user awareness, etc, as well as identifying the key challenges in ISM implementation.
(Muratha)	Research paper	Contingency theory	Information security practices in the Kenyan capital market. Human remains the weakest link in achieving information security.	The study by Muratha (2012) carried out in Kenya, focused on the practices of information security on capital markets (a survey of several commercial banks). The purpose was to establish the information security breaches and find out the practices adopted.

				My study focuses on the challenges being faced during implementation of the security practices and strategies and how to address these challenges in KenGen.
(Dhillon and Backhouse)	Research Paper	Critical theory	Proper implementation of ISM can be achieved through establishing formalized rules, policies and new technology.	This study by Dhillon & Backhouse (2000) highlighted the drivers of ISM strategy implementation most of which are the moderating variables in the Kenyan setting like the government policies, organization procedures and standards. My study will focus on to what extend these drivers affect ISM strategy implementation in KenGen.
(Stulz)	Conceptual Paper	Theory of risk management	Risk management as a core driver in achieving information security.	Stulz (1996) conceptual paper focused on only risk management as a driver of information security. My study focuses on to what extent, the other main drivers like strategic alignment alongside risk management affect ISM strategy implementation and the challenges involved in ISM strategy implementation.

Appendix IV: List of Power Generating Companies in Kenya

1. Kenya Electriciry Generating Company

2. Tsavo Power Company

3. OrPower

4. Iberafrica

5. Rabai Power