FACTORS INFLUENCINGPOST IMPLEMENTATION SYSTEM SECURITY OF MANAGEMENT INFORMATION SYSTEMS: A CASE STUDY OF NAIROBI CITY WATER AND SEWERAGE COMPANY, NAIROBI COUNTY, KENYA

BY

GLADYS WAMBUI NJOROGE

A RESEARCH PROJECT REPORT SUBMITTED IN FULFILMENT OF THE DEGREE OF MASTERS OF ARTS IN PROJECT PLANNING AND MANAGEMENT AT THE UNIVERSITY OF NAIROBI.

2013

DECLARATION

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

Signed …… Date ……..

GLADYS WAMBUI NJOROGE

L50/60567/2010

This research project has been submitted for examination with my approval as the candidate's University Supervisors.

Signed …… Date ……..

PROF. CHRISTOPHER GAKUU

Department of Extramural Studies

DEDICATION

This study is dedicated to my loving family, for their support, encouragement and patience during the entire period of my study and continued prayers towards successful completion of this course.

ACKNOWLEDGEMENT

I would like to express my sincere thanks to the supervisor Prof. C. M. Gakuu for supervising this research paper and his patience in reading the drafts and occasionally guiding me, without which the research would not have been a reality.

I wish to express my sincere appreciation to the University of Nairobi, specifically the Department of Extra Mural studies, for providing the facilities for the research and the lecturers.

TABLE OF CONTENTS

Page

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS AND ACORONYMS

B2B	-	Business-To-Business
B2C	-	Business-To-Consumer
CMS	-	Customer Management System
DMS	-	Document Management System
DOS	-	Denial of service
DTI	-	Department of Trade and Industry
ERP	-	Enterprise Resource Planning
GIS	-	Geographical Information System
HRMS	-	Human Resource Management System
ICT	-	Information Communication System
ISACA	-	Information Systems Audit and Control Association
MIS	-	Management Information System
NCWSC	-	Nairobi City Water and Sewerage Company
PDAs	-	Personal Digital Assistants
SPA	-	Service Provision Agreement
SPMS	-	Stores and Procurement Management System

ABSTRACT

Security is a pre-requisite for any IT undertaking in a company. Although post-implementation activities are critical for the acceptance of and security of the management information systems (MIS), post-implementation strategies are, however, not emphasized in most MIS projects, because conventional project management methodologies consider that a project is over when the system or facility is operating. Requirements of MIS tend to change continuously even after the completion of the project. Some factors that pose as the greatest challenge after the implementation of management information systems include lack of senior management commitment to information security initiatives, failure of management to understand the information security issues, lack of information security planning prior to implementation of new technologies and lack of Integration between business and information security. The purpose of this study was to assess the factors effecting system security post implementation of management information system at NCWSC. The propose study adopted a case since it is a research on one organization. The target population of this study was the one hundred and twenty one management staff working at NCWSC. Stratified proportionate random sampling technique was used to select the sample of 30 managers. The study used both primary and secondary data. Primary data was obtained through self-administered questionnaires with closed and open-ended questions and an interview schedule. A descriptive analysis was employed in analyzing the quantitative data. Content analysis was used for data that is qualitative nature or aspect of the data collected from the open ended questions and the interview guides. The study found that system environment and database exposure affected information system security in the company to a very great extent (65%). It was clear that the quality of the software application(MIS) affected information system security in the company to a very great extent (75%) and end user effect affected information system security in the company to a very great extent (70%). The study concludes that MIS effectiveness is a function of environmental factors, design factors i.e. the quality of the software, the system end users and internal and external processes. The study recommends that companies should develop and implement a good information systems policy to ensure quality control of the data stored in their system.

CHAPTER ONE

INTRODUCTION

This chapter contains the background, problem statement, objectives of the study and the research questions of the proposed study. It also covers the significance of the study, scope and definition of key terms.

1.1 Background of the Study

The adoption of Information Systems (IS) in many businesses is at a fast tempo in order to remain more competitive (Norman and Yasin, 2010). This fast adoption is very much supported by the rapid technology advancement and the increasing demand from business stakeholders. Many organizations in developed and developing countries -in both private and public sectors- turn to Information Technology/Information Systems (IT/IS) to meet the increasing demands on organizations to increase their efficiency and effectiveness. In the era of the information society, the development and application of information technology proceeds relentlessly. The management of information technology (IT) projects is a challenging task with many projects failing to achieve their intended objectives. Many organizations do not critically examine the causes for project failure and this prevents them from learning from their mistakes. At the same time, technological innovations bring in their wake new technical and managerial concerns over security. For educators in the field of information systems security (ISS), this has a profound impact on many organizations operations and performance.

Organizations of all shapes and sizes have to enthusiastically embrace information systems and technologies if they wish to survive and, better still, thrive in a highly competitive environment,

in which effective operational control and strategic direction are increasingly dependent on the availability and exploitation of high quality information. Consequently, it is vital that adequate security and control procedures are introduced to ensure that all the information embedded within organizational information systems retains its integrity, confidentiality and availability (Dhillon and Backhouse, 2009). However, there is also extensive evidence to suggest that the threats, to the security of organizational information and information systems, are now growing in number, variety and, most importantly, the severity of their impact. For example, traditional threats to the security of information and systems include: natural disasters, theft of hardware/software, unauthorized access and human error, while newer threats include viruses and hacking and cyber terrorism (Furnell and Warren, 2009).

Computer users face fundamentally new levels of risks in information security after implementation of management information systems because of increased use of networks, increased computer literacy, an explosion in microcomputer use and decentralized data processing capabilities, and increased dependency on information technology overall. Realizing this fact is considerably easier than taking action to ease these risks, for computer security is fraught with hidden problems and contradictions. For example, while teenaged hackers have brought computer security and crime to the attention of policymakers and the public, most systems can be protected from hackers rather easily. The abuse of computer systems by those authorized to use them, as well as such mundane issues as protection from operator errors and natural or man-made disasters are more difficult problems. The Federal Government's experience in this area provides a number of lessons that are applicable to the private sector as well.

Information system security processes and activities provide valuable input into managing IT systems and their development, risk identification, planning and mitigation. A risk management approach involves continually balancing the protection of agency information and assets with the cost of security controls and mitigation strategies throughout the complete information system development life cycle (Wider and Davis, 2008). Implementing information security early in the project allows the requirements to mature as needed and in an integrated and cost-effective manner.

To a very large extent, such threats after implementation of management information systems are growing because of higher levels of interconnectivity both within and between organizations (Laudon and Laudon, 2010). In particular, it is the increasing incidence of intra-organizational systems that is creating problems for organizations, as information security is upgraded from being merely a "domestic" issue to one that involves third parties, such as external business partners. The rise of electronic commerce has also heightened awareness among organizations of the security threats to which they are likely to be exposed. Indeed, it has been reported that security threats, and fear of security breaches, constitute the greatest inhibitors to an expansion in the uptake of electronic commerce. Increased interconnectivity is not, however, the only factor making computers, and the information therein, less secure. For example, the widespread recognition that information now constitutes a "key corporate asset", which is of great commercial value, has also brought information security nearer to the top of the management agenda.

Advanced technology has created significant risks related to ensuring the security and integrity of Information Systems (Rajendra and Ajay 2011). Perhaps inevitably, the increased risk of

information security problems has led to a growing awareness among the managers of organizations of the need for careful and effective information security management. For example, it is widely acknowledged that effective information security management after implementation is dependent on a number of key factors, most notable among these being: the need for senior management commitment and support to information security management; the detailed assessment of potential security risks and threats; the implementation of appropriate controls to minimize or guard against those risks and threats; and the thorough communication of security issues to users of both information and information systems through relevant education and training. Due to the high-tech nature of these systems and the technological expertise required to develop and maintain them, it is not surprising that overwhelming attention has been devoted by computer security experts to technological vulnerabilities and solutions.

For management information systems post-adoption in particular, user companies may inevitably be confronted with a wide range of risks when exploiting and optimizing their implemented systems. This is particularly true, considering three apparent facts. Firstly, some failures (e.g. insufficient user training) are prevalent in the implementation, even if the implementation project itself is considered a successful one. Such initial failures can inevitably cause severe problems in MIS post-implementation. Secondly, undesirable internal and external changes (e.g. high attrition rate of information technology (IT) experts, system vendor related issues) may arise over time, and can directly impact the use of implemented MIS systems. Thirdly, internal and external barriers (e.g. poor communication between functional divisions, unstable business environment) existing in the business context may prevent companies from achieving long-term MIS success. The occurrence of undesirable risks in the post-implementation stage will not just

turn the initial MIS success into a failure, but may also lead to significant system and business disasters (Azah and Norizan 2010).

However, it has also been recognized that effective security management, including all the above factors, is predicated on the formulation, dissemination and operation of an information security policy. Layton (2007) acknowledges that one of the most important controls is the information security policy, while Higgins (2009) notes that the information security "policy is the start of security management".

Importance of the information security policy, as a document of strategic importance within organizations today, is widely acknowledged. Indeed, in the UK, the British Standards Institute has developed a standard. Moreover, the issue of information security policies has now become an integral part of a variety of commercial surveys into information security breaches and safeguards (Ernst and Young, 2008). However, there is little evidence that any empirical research, specifically targeting the uptake, dissemination and impact of information security policies within organizations, has been conducted and published in the academic literature.

Despite the focus on IT project security success and failure by researchers there has been relatively little attention given to how individuals attribute IT project security success and failure. It has been suggested that during declining information security, top managers who attribute insecurity to internal sources as opposed to external sources are more likely to show greater levels of strategic reorientation. How people attribute success and failure of an information management system on an individual basis is likely to have a significant impact on the organizational perception of the final assessment of a project (Maroukian, 2010).

1.1.1 Nairobi City Water and Sewerage Company

According to the Nairobi City Water and Sewerage Company's (NCWSC) four year Strategic Business Plan that became operational in 2007, the company, also known as the Nairobi Water Company (NWC) was formed in line with the Water Sector Reforms under the Water Act 2002. The company has been licensed by the AWSB to provide water and sewerage services to the people of Nairobi and its environs. The license is based on an agreed framework specified in the Service Provision Agreement (SPA) that ensures adequate and quality supply of water, affordable tariffs, and maintenance and improvement of water and sewerage infrastructure.

The company in its three year strategic plan 2007/8 – 2009/10 recognizes the tremendous role that ICT has to play in meeting the laid down goals. Implementation of several integrated systems that comprise of Oracle Financials for Accounting and Financial Management, Stores and Procurement Management System (SPMS) for the supply chain, Human Resource Management System (HRMS), Geographical Information System (GIS), Fleet management, Document Management System (DMS) and the Customer Management System (CMS) have been completed and enhancement continuously done in order to meet the organizational demands. Several other related projects have been initiated, but it is the CMS project that has so far received the greatest level of investment among all these systems.

In order to improve the organizations operational efficiency in meter reading the company has heavily invested in data loggers, ICT equipments that the meter readers log in data in the field and upload in the CMS when they return back from the field. In addition, the GIS has assisted in mapping routes and put together meters that can be read in a day easily into manageable clusters called Itineraries. This investment has resulted in a reduction of erroneous data entry, shorter

billing cycle that is the time taken from the date the meter is read to the time the bill (invoice) is dispatched.

The Organization implementation of the procurement and stores systems has greatly improved procurement cycle and services of the stores as well as ensuring that the stock items are well managed. Its seamless integration with the Oracle Financials further ensures that suppliers' data is accessible to the financial system without paper or files being pushed, this has minimized document losses which were a major problem during the manual systems operations.

1.2 Statement of the Research Problem

Security is a pre-requisite for any IT undertaking in a company. Although post-implementation activities are critical for the acceptance of and security of the management information systems, post-implementation strategies are, however, not emphasized in most MIS projects, because conventional project management methodologies consider that a project is over when the system or facility is operating (Rajendra and Ajay, 2011). Requirements of MIS and structures tend to change continuously even after the completion of the project.

Indeed, MIS is of great strategic importance to most companies. However, no system can be made absolutely secure. As information systems (IS) have become more prevalent in business, the consequences of Information System Security (ISS) violations have become more and more costly. Olivia (2004) states that with constantly increasing technical complexity, legal barriers and privacy expectations, the challenges of information security have risen exponentially in the past five years. Information Systems Audit and Control Association (ISACA) (2005) has summarized several factors that pose as the greatest challenge after the implementation of

management information systems. Some of these are; lack of senior management commitment to information security initiatives, failure of management to understand the information security issues, lack of information security planning prior to implementation of new technologies and lack of Integration between business and information security.

Calder (2005) states that there are a number of trends that lie behind the increases in threats to information security, which, when taken together, suggest that things will continue to get worse, not better. Better hacker tools are available every day, on hacker websites that, themselves, proliferate. These tools are improved regularly and, increasingly technologically proficient criminals and computer literate terrorists are thus enabled to cause more and more damage to target networks and systems. Olivia (2004) concludes that IT executive and senior management must retain a vigilant posture concerning information security, as the impact of a successful attack or theft can be devastating to customers and the organization in terms of loss of customer trust, unreliable information and corrective action expenses.

A survey by Ernst and Young (2008) that focused on corporation in US found that more than 75 percent of business had experienced some interruption of their critical business systems related to IT security. The global economic impact of information security is high and this calls for extensive research in the field of information security especially in the Kenyan public sector with a view of identifying the factors that affect security after implementation of MIS. Obara (2010) observed that there are many ISs security issues in Kenyan state parastatals while Gichuru (2000) indicated that computer security systems at the University of Nairobi are affected by physical infrastructures, accessibility, data security, and intrusion through the network. Nairobi City Water and Sewerage Company is not an exception. Security of information is therefore of

paramount importance especially to the public sector and this forms the motivation behind the study to assess the factors affecting security of management information system after they are implemented with specific reference to Nairobi City Water and Sewerage Company

1.3 Purpose of the Study

The purpose of this study was to assess the factors affecting system security post implementation of management information system at Nairobi City Water and Sewerage Company.

1.4 Objectives of the Study

The study was guided by the following specific objectives.

i. To establish how the system environment influences post implementation security of management information system at Nairobi City Water and Sewerage Company

ii. To establish the extent to which after sale services by the vendor influences post implementation security of management information system at Nairobi City Water and Sewerage Company

iii. To determine how the database exposure influences post implementation security of management information system at Nairobi City Water and Sewerage Company

iv. To assess the influence of the quality of software applications on post implementation security of management information system at Nairobi City Water and Sewerage Company

v. To establish how the end users affects post implementation security of management information system at Nairobi City Water and Sewerage Company

1.5 Research Questions

The following research questions were answered:

i. How does the system environment influence system security post implementation of management information system at Nairobi City Water and Sewerage Company?

ii. To what extent does after sale services by the vendor influence system security post implementation of management information system at Nairobi City Water and Sewerage Company?

iii. How does the database exposure influence system security post implementation of management information system at Nairobi City Water and Sewerage Company?

iv. To what extent is the influence of quality of the software applications on system security post implementation of management information system at Nairobi City Water and Sewerage Company?

v. What is the extent to which the end users influence system security post implementation of management information system at Nairobi City Water and Sewerage Company?

1.6 Significance of the Study

This study offers valuable contributions from both a theoretical and practical standpoint. From a theoretical standpoint, it contributes to the general understanding of factors affecting security of management information system after they are implemented. The study is invaluable to the following:

It will be important to the management at the Nairobi City Water and Sewerage Company as they will get a better understanding of the challenges they are likely to face after implementing management information system and the factors that are likely to cause the same.

The research findings will also provide vital information that will assist government particularly policy makers, planners and programme implementers to formulate policies and strategies on management information system.

The study will also be invaluable to information systems security consultants and information systems auditors as the study will pin point areas that need to be addressed in the implementation of information security in the public sector.

The research findings will also provide vital information that will benefit future academicians and researchers on factors affecting security of management information system after they are implemented. It will also add on to the existing body of knowledge in the area of information security. Thus, academics will use this study as a basis for further research on the area.

1.7 Delimitation of the Study

This study set out to analyze the factors effecting system security post implementation of management information system at Nairobi City Water and Sewerage Company. The study was limited to five variables that is, system environment, after sale services by the vendor, database exposure, quality of software applications and end users. The study was carried out in Nairobi City Water and Sewerage Company headquarters where the managers were the main respondents.

1.8 Limitations of the Study

The study encountered time constrain as the period allocated for the study is limited and has to combine the study and work given that the researcher is employed. The study therefore focuses on a small proportion of the total population as a representative of all the possible respondents. The study also encounter financial constrains in the research process given that the researcher is self sponsored.

1.9 Definition of Significant Terms

Information security - This means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction

Management Information System–a computerized system providing management with accurate and timely information necessary to facilitate the decision-making process and enable the organization's planning, control, and operational functions to be carried out effectively.

System Environment – This is the physical environment where the management information system is installed i.e. the server rooms, that may affect the effectiveness of the management information system

1.10 Organization of the Study

The study is organized into five chapters. Chapter one contains the introduction to the study. It presents background of the study, statement of the problem, purpose of the study, objectives of the study, research questions, significance of the Study, delimitations of the study, limitations of the Study and the definition of significant terms. On the other hand, chapter two reviews the literature based on the objectives of the study. It further looked at the conceptual framework and finally the summary. Chapter three covers the research methodology of the study. The chapter describes the research design, target population, sampling procedure, tools and techniques of data collection, pre-testing, data analysis, ethical considerations and finally the operational definition of variables. Chapter four presents analysis and findings of the study as set out in the research methodology. The study closes with chapter five which presents the discussion, conclusion, and recommendations for action and further research.

CHAPTER TWO

LITERATURE REVIEW

2.1 Introduction

This chapter summarizes the information from other researchers who have carried out their research in the same field of study. This literature review commences with an assessment of some recent surveys into the key issues surrounding information security, which provides a useful context for study, before focusing more specifically on the factors affecting security of management information system after they are implemented. The section concludes with a conceptual framework.

2.1.1 Management Information System

MIS is an organized approach to the study of the information needs of an organization's management at every level in making operational, tactical, and strategic decisions. Its objective is to design and implement procedures, processes, and routines that provide suitably detailed reports in an accurate, consistent, and timely manner (Knight, 2009).

The term “management information system” (MIS) is synonymous with computer-based systems. Used broadly, it is seen as the system satisfying all the information needs of managers. MIS is the study of providing information to people who make choices about the disposition of valuable resources in a timely, accurate, and complete manner at a minimum of cognitive and economic cost for acquisition, processing, storage, and retrieval. Another definition emphasizes the use to which the information is put, rather than the way it is produced: A system to convert

data from internal and external sources into information and communicate that information in an appropriate form, to managers at all levels in all functions to enable them to make timely and effective decisions for planning, directing and controlling the activities for which they are responsible (Bee and Bee, 2010).

In a management information system, modern, computerized systems continuously gather relevant data, both from inside and outside an organization. This data is then processed, integrated, and stored in a centralized database (or data warehouse) where it is constantly updated and made available to all who have the authority to access it, in a form that suits their purpose. There are so many definitions of MIS. For the purpose of this research, MIS can be defined as a system providing management with accurate and timely information necessary to facilitate the decision-making process and enable the organization's planning, control, and operational functions to be carried out effectively. So in this way, management information systems increase competitiveness of the firm by reducing cost and improving processing speed.

A management information system (MIS) provides information which is needed to manage organizations efficiently and effectively (Laudon and Laudon, 2010). Management information systems involve three primary resources: people, technology, and information or decision making. Management information systems are distinct from other information systems in that they are used to analyze operational activities in the organization. Academically, the term is commonly used to refer to the group of information management methods tied to the automation or support of human decision making, e.g. decision support systems, expert systems, and executive information systems.

2.1.2 Information Security

Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction (Layton, 2007). According to Calder (2005, the use of distributed computing is increasing. Computing power has migrated from centralized mainframe computers and data processing centers to a distributed network of desktops, laptops and micro-computers. There is a strong trend towards mobile computing. The use of laptop computers, Personal Digital Assistants (PDAs), mobile phones, digital cameras, portable projectors and MP3 players has made working from home or on the road relatively straightforward, with the result that network perimeters have become increasingly porous. There are many more remote access points to networks, and the number of easily accessible endpoint devices has increased dramatically, increasing the opportunities to break into networks and steal or corrupt information.

As Wylder (2004) observes, there has been a dramatic growth in the use of the internet for business communication, and the development of wireless, VoIP and broad-band technologies will drive this even further. He asserts that there is widespread computer literacy. While most people today have computer skills, the next generation is growing up with a level of familiarity with computers that will enable them to develop and deploy an entirely new range of threats.

Dhillon and Backhouse (2009) states that security can be defined as the state of being free from danger and not exposed to damage from accidents or attack, or it can be defined as the process for achieving that desirable state. The objective of information system security is to optimize the performance of an organization with respect to the risks to which it is exposed. Business is becoming increasingly dependent on technology and the internet to the point where some

businesses would come to a screeching halt if they did not have it. This is particularly true in larger companies, where the ability to communicate and access information is the lifeblood of the business. The internet provides an effective, immediate and powerful method for organizations to communicate on all sorts of issues. This exposes all these organization to the security risks that go with connection to the internet.

According to Kairab (2005), the need to secure information is becoming greater all the time as we leverage technology to automate functions, as more data becomes electronic, and as companies become increasingly reliant on the internet as an integral part of their information technology (IT) infrastructure. Businesses are becoming increasingly connected because business to business relationships are helping companies drive efficiencies and shorten the supply chain. E-commerce is gaining acceptance as more people buy goods and services online, resulting in an increasing number of companies having a presence on the Web. With these relationships, a host of security issues must be addressed.

According to Peltier (2005), an effective information security program endeavors to ensure that the organization's information and its processing resources are available when authorized users need them. It must take into account the business objectives and the mission of the organization and ensure that these goals are met safely and securely as possible. Understanding the customer's needs must be the first step in establishing an effective information security program. Information security is not only a technical issue, but a business and governance challenge that involves adequate risk management, reporting and accountability. As Information Technology Governance Institute (2006) puts it, effective security requires the active involvement of executives to assess emerging threats and the organization's response to them.

According to McCumber (2005) the art and science of security requires a complete understanding of the value of the assets requiring protection. The asset under scrutiny is primarily the information transmitted, stored, and processed by the organization. Secondarily, the computer and telecommunications resources themselves require protection. The goals of Information security are to ensure the confidentiality, integrity and the availability of data within a system. The data should be accurate and available to the appropriate people, when they need it, and in the appropriate condition. Warkentin et al (2006) notes that perfect security is not feasible, instead IT security managers strive to provide a level of assurance consistent with the value of the data they are asked to protect.

Information Technology Governance Institute (2006) argues that an enlightened approach to information security takes the larger view that an organization's information and the knowledge based on it must be adequately protected regardless how it is handled, processed, transported or stored. It addresses the universe of risks, benefits and processes involved with all information resources. The security of information, as with other critical organizational resources, must be addressed at the total enterprise level. It further argues that as banks strive to remain competitive in the global economy, they respond to constant pressures to cut costs through automation, which often requires deploying more information systems. Whilst managers become ever more dependent on these systems, the systems have become vulnerable to a widening array of risks that can threaten the existence of the enterprise. This combination is forcing management to face difficult decisions about how to effectively address information security. This is in addition to scores of new and existing laws and regulations that demand compliance and higher levels of accountability.

Calder et al (2005) assert that security of information systems is necessary because the threats to the availability, integrity and confidentiality of the organization's information are great, and always increasing. All organizations possess information, or data, that is either critical or sensitive. In the Information Security Breaches Survey 2004, the United Kingdom Department of Trade and Industry commented: ‘information is widely regarded as the lifeblood of modern businesses’. According to a 2000 DTI survey, 49 per cent of organizations believe that information is critical or sensitive because it will be of benefit to competitors, while 49 per cent believe that it is critical to maintaining customer confidence. The 2004 survey identified the fact that, while 58 per cent of all businesses had highly confidential information stored on their computer systems, 77 per cent of large businesses were in this category. Two other findings of the 2004 survey indicate the extent to which UK businesses are dependent on electronic information: roughly nine-tenths of them now send e-mail across the internet, browse the web and have a website; and 87 per cent of businesses now identify themselves as ‘highly dependent’ on electronic information and the systems that process it, compared to 76 per cent in 2002.

Organizations are facing a flood of threats to this information. It is self-evident that organizations should, therefore, take appropriate steps to secure and protect their information assets. This is particularly so because, as Osborne (2006) asserts, a web of legislation and regulation makes firms criminally liable and, in some instances, makes directors personally accountable, for implementing and maintaining appropriate risk control and information security measures.

Olivia (2004) argues that information security is no longer an “event” or part-time assignment for corporate and government organizations rather it has become a continuous process every second of every day, from both the technology and management perspectives. Most executives

of small companies are unaware that their corporate firewall is probed hundreds of times a day by automated attack tools. Financial services and government firewalls are often probed tens of thousands of times every day.

According to Garg et al (2003), without a doubt, information security is a pervasive concern for all companies and continues to rise in importance. It is now considered a mainstream operational concern as companies utilize the Internet as a key driver of e-business and greater collaboration. While the exigencies of e-commerce require that the internet be safe and secure, the reality is drastically different. As adoption and dependence on the internet grows, electronic collaboration will accelerate rapidly as organizations see the impact on their bottom lines. However, concerns over security and associated issues continue to be listed as a top challenge, hindering the multibillion dollar potential of B2B (business-to-business) and B2C (business-to-consumer) opportunities.

In addition to the growth of E-commerce, several significant changes driven by the forces of globalization and the regulatory environment make information security an even greater area of concern. Examples of such laws include the HIPAA (2010), COPPA (2009), and Gramm-Leach-Bliley Act (2010), SOX (2002), Other pieces of UK legislation that are relevant to information security include Copyright Designs and Patents Act (2008); the Computer Misuse Act (2007); the Data Protection Act (2009); the Human Rights Act (2009); the Electronic Communications Act (2000); the Freedom of Information Act (2000); Regulation of Investigatory Powers Act (2000); the Privacy and Electronic Communications Regulations (2003) that require thorough safeguards to protect the security and confidentiality of data, individual medical records, and the privacy of children on the Internet.

Sookdawoor (2005) argues that computer systems and the information processed on them must be considered critical assets that support the mission of an organization. Protecting them can be as important as protecting other organisation resources such as financial resources, physical assets, and employees. The costs and benefits of information protection should carefully be examined in both monetary and non monetary terms to ensure the cost of controls does not exceed expected benefits. Information protection controls should be appropriate and proportionate.

Today, as Bosworth et al (2002) puts it, information systems are much larger and more widely distributed, interconnected, and interdependent, and the risks are many times greater. So too are the potential costs of any IS disruption. Data processing, transmission, and storage now occur throughout the premises and far beyond. Many and diverse intra- and interoffice transmission media exist, and still more that may connect a vast number of remote sites. The infrastructure has become much harder to protect.

2.1.3 Information Security Policy

As noted in the introduction, there is a growing recognition that effective information security management is predicated on the existence and execution of an information security policy. As Eisenhardt (2009) notes, “without a policy, security practices will be developed without clear demarcation of objectives and responsibilities”. However, there is also a growing concern that too many organizations are failing to heed this advice, as witnessed by the low levels of uptake of formal information security policies (Arnott, 2002), and the inadequacies in policies, where they do exist (Moule and Giavara, 2009; Hone and Eloff, 2002). While the importance of, and

concerns about, information security policy are widely recognized, this interest has not, as yet, been translated into detailed empirical surveys explicitly targeting the utilization of information security policies in organizations. However, some interesting insights about information security policy can be gained from a number of more general studies of information security.

Each study explored the prevalence and range of security incidents experienced by European organizations in the past couple of years, and all three concluded that there is an upward trend in the number of incidents occurring and in the severity of individual incidents. More importantly, perhaps, the studies also explicitly investigated the uptake of information security policies. For example, the Andersen (2001) study reports that 65 percent of the organizations surveyed (most of which were large organizations) had an information security policy in place, and the Department of Trade and Industry (DTI) (2002) survey reports that 27 percent of UK businesses have a policy in place. The DTI study further reports that 59 percent of the large organizations surveyed had implemented a policy. Significant in these DTI results is that again an upward trend is noted from earlier studies: the DTI (2000) study, for example, reported that only 14 percent of the organizations surveyed had an information security policy in place. Moreover, the 2002 study noted that a higher proportion of organizations with a policy were undertaking annual policy updates than was the case in 2000.

The Andersen (2001) study is of particular interest, as it highlights the discrepancy between the views of business managers and those of IT managers: 82 percent of the business managers surveyed believed that their organization had a comprehensive policy in place, whereas only 66 percent of the IT managers believed this to be the case. This could suggest that a survey targeting IT managers, who presumably typically have a more detailed knowledge of information security

issues than business managers, is likely to yield a more realistic assessment of the information security situation in an organization.

The Ernst and Young (2001) survey found that organizations believed “employee awareness” to be the greatest “challenge to achieving the required level of security”, a message that is strongly echoed by Siponen (2000). Given this finding, it seems somewhat disconcerting that, of the 27 percent of organizations in the DTI (2002) survey having an information security policy, only 7 percent of them implemented their policy in order to make employees aware of security issues. The primary motivation for having a policy (as reported by 67 percent of organizations that have a policy) was the recognition that it is considered to be “good practice”. It was further reported in the DTI (2002) survey that few organizations make their employees aware of information security issues on induction. It seems, therefore, that, while policy formulation might be on the increase, an emphasis on dissemination of security concerns to employees and practical policy implementation is very low on the agenda of many organizations.

The studies undertaken to date have not investigated the specific areas covered by the information policies organizations have adopted, nor do they appear to have considered the specific impact those policies are having in organizations (Eisenhardt, 2009;Guilfoyle, 2000). A strong indication of the paucity of research in the area of information security policy is provided by Dhillon and Backhouse (2001). Their comprehensive review of the information security literature concluded that existing research tends to focus on “check-lists (of security controls), risk analysis and evaluation”; information security policy was not explicitly featured in their review. Consequently, fewer or no empirical data exist on the important issues of policy uptake, content and implementation.

The DTI (2000) survey reported that only 25 percent of the UK businesses surveyed were aware of the existence of this standard. Moreover, the DTI, in their 2002 survey, expressed disappointment that only 15 percent of organizations were aware of the contents of this standard, and only 38 percent of those aware of its contents had actually adopted the standard in their organization. These low levels of awareness are particularly disappointing, given that the standard has been in existence since 2009.

The standard contains a number of factors cited as critical to the success of information security management in organizations, such as ensuring the policy reflects business objectives, effective marketing of security to employees, provision of security training, and policy performance measurement. To date, despite the existence of the major studies of security issues mentioned in this paper, there seem to be few empirical data to indicate whether organizations are adopting these individual factors, or on the impact the adoption of these factors is having on information security in organizations. It should be noted that, while this literature review and our study have both focused upon the BS 7799 standard, the work has far wider international relevance, as the British Standard became an international standard in 2000: ISO 17799 (ISO, 2000).

2.2 Theoretical Orientation

2.2.1 Agency Theory

Agency theory is directed at the ubiquitous agency relationship, in which one party (the principal) delegates work to another (the agent), who performs that work. Agency theory is concerned with resolving two problems that can occur in agency relationships. The first is the agency problem that arises when (a) the desires or goals of the principal and agent conflict and

(b) it is difficult or expensive for the principle to verify what the agent is actually doing. The problem here is that the principal cannot verify that the agent has behaved appropriately. The second is the problem of risk sharing that arises when the principal and agent have different attitudes towards risk. The problem here is that the principle and the agent may prefer different actions because of the different risk preferences (Eisenhardt, 2009).

Agency theory describes the theoretical roots of the problems that principles-based executive compensation was designed to solve. Agency theory examines the relationship between the principal (the Shareholders) and the agent (the CEO)—who has been engaged to make decisions on the principal's behalf. Issues may develop because the principal and agent, while working toward the same goal, do not always share the same interests. This is a theory explaining the relationship between principals, such as a shareholders, and agents, such as a company's executives. In this relationship the principal delegates or hires an agent to perform work. The theory attempts to deal with two specific problems: first, that the goals of the principal and agent are not in conflict (agency problem), and second, that the principal and agent reconcile different tolerances for risk.

Agency theory explains how to best organize relationships in which one party (the principal) determines the work, which another party (the agent) undertakes (Eisenhardt, 2009). The theory argues that under conditions of incomplete information and uncertainty, which characterize most business settings, two agency problems arise: adverse selection and moral hazard. Adverse selection is the condition under which the principal cannot ascertain if the agent accurately represents his ability to do the work for which he is being paid. Moral hazard is the condition

under which the principal cannot be sure if the agent has put forth maximal effort (Eisenhardt, 2009).

The problems of adverse selection and moral hazard mean that fixed wage contracts are not always the optimal way to organize relationships between principals and agents (Jensen and Meckling, 1976). A fixed wage might create an incentive for the agent to shirk since his compensation will be the same regardless of the quality of his work or his effort level (Eisenhardt, 2009). When agents have incentive to shirk, it is often more efficient to replace fixed wages with compensation based on residual claimancy on the profits of the firm (Alchian and Demsetz, 1972). The provision of ownership rights reduces the incentive for agents' adverse selection and moral hazard since it makes their compensation dependent on their performance (Jensen, 1983).

A number of scholars have shown that the problems of adverse selection and moral hazard exist in the management of retail outlets (Rubin, 1978; Mathewson and Winter, 1985; Brickley and Dark, 1987). Outlet managers have an incentive to shirk and to misrepresent their abilities since the owner of the firm cannot easily differentiate the effect of manager behavior on outlet performance from the effect of exogenous factors (Carney and Gedajlovic, 2007). Franchising scholars have found that one way that performance of retail outlets can be enhanced is through the provision of residual claimancy that comes from franchising (LaFontaine and Kauffman, 2006).

2.2.2Stakeholder Theory

A stakeholder is defined as, “any group or individual who can affect or is affected by the achievement of the organization's objectives” (Freeman, 1984, p. 25). The application of stakeholder theory provides methods for identifying and managing stakeholder goals and objectives, which is done from two perspectives: inside-in and inside-out (Freeman, 1984). The inside-in perspective considers actors internal to the company (i.e. employees, managers), while the inside-out view looks at groups connected to the organization, but to a lesser degree and in a different capacity (i.e. shareholders). As a method to facilitate organizational change, stakeholder perspective is well-supported. As noted by Haberberg and Rieple (as cited in Lovegrove, 2005), stakeholder approach is based on three basic declarations: organizations possess a number of constituencies that affect and are affected by others; the interactions and the outcomes of processes undertaken by these groups affects the organization as well as other stakeholder groups; stakeholder perceptions affect the viability of strategic action. The introduction of an MIS is one such example of a strategic action that is also a change initiative. It is a commonly held belief that without engagement and acceptance by stakeholders, it is unlikely that any change will deliver the potential benefits promised. Therefore, it can be clearly justified that stakeholder consultation is a necessary element of any change management program.

A look more specifically, at the stakeholder literature in the information system (IS) field reveals that identified stakeholder groups have included managers, IT professionals, end-users, and internal auditors (Infinedo and Nahar, 2007). Lyytinen, Mathiassen and Ropponen (as cited in Infinedo and Nahar, 2007), however, believe that stakeholders can be identified based on research purpose, or more particularly as actors that can set forth claims or benefit from IT

systems development issues. Therefore, depending on the situation, identified stakeholders may extend to broader groups. More particularly in the (management information system) MIS field, Legris and Collerette (2006) have introduced a table summarizing the MIS implementation process and have identified stakeholders as project managers, vendors, users and system owners. Similarly, Akkermans and van Helden (2002) also include project managers and vendors, but they add project champion and top management to that group. External to the company, however, there are other groups to consider, such as customers, suppliers and business partners (Bajwaet al., 2004). These differences demonstrate how, as noted above, the nature or purpose of the research will determine the stakeholder groups considered.

A review of the literature has also provided insight into documented differences in stakeholder perspective. For instance, it has been suggested by Grindley (as cited in Infinedo and Nahar, 2007) that due to cultural differences, some of the identified groups will hold conflicting views on IT related issues. Several studies have explored this dimension. Particularly, Schein (2006) concluded that top management and IT personnel belonged to distinct subcultures. Similar research by Ward and Peppard (2010) revealed cultural gaps between IT and business departments. One of the reasons cited for the divergence between these two groups extends to different goals regarding IT issues. In the domain of ERP, research by Singletary et al. (as cited in Infinedo and Nahar, 2007) has revealed differences between managers, IT professionals and end-users on benefits and drawbacks of MIS implementation. Finally, work by Bradley and Lee (2004) has revealed discrepancy between technical and management personnel regarding understanding of necessary levels of training. This kind of research is limited, however, as the majority of study has been managerially focused and the stakeholder perspective has not been often considered (Amoako-Gyampah, 2004). Kossek's (2007) work brings attention to the need

to consider the perceptions of other important groups and Amoako-Gyampah (2004, p. 171) more specifically states that knowledge of any differences can “help implementers develop appropriate intervention mechanism such as training and communication that can lead to successful MIS implementation”.

2.3The System Environment and Security of the Management Information System

According to Cohen and Bailey (2008), MIS effectiveness is a function of environmental factors such as industry characteristics and turbulence. Environmental factors, design factors, employees’ psychological traits and internal and external processes can predict the MIS effectiveness. The turnover in the industry, at the managerial level, can also affect the performance of software development teams in the organization. Ebert and Neve (2001) stated that work environment and effective and efficient tools are some of the glues for global software development projects. The distribution of software development globally results into multicultural engineers work together results into innovative products and processes.

The company’s policies and standards must require review and formal authorization of changes to the technology environment prior to implementation. The designation of authority to provide such authorization should be of management position, without separation of duties conflicts, and responsible for reporting the status of information security to the board. Exceptions to the company’s policies and standards with regard to change management should be formally requested and approved by the company’s policy oversight committee or equivalent. Measurements of control effectiveness should include alignment with regulation and law and those measurements should be reported to the board on a quarterly and annual basis through, or with, the chief legal counsel, chief compliance officer, and chief auditor or their equivalents.

Schifreen (2006) supports by noting that every company needs a formal written document which spells out to staff precisely what they are allowed to use the company's systems for, what is prohibited, and what will happen to them if they break the rules. This document is known as an information security policy.

Ross (2007) also supports this by arguing that the ideal situation is for the security of the system to be self enforcing. To some extent, this is currently a reality. Firewalls, intrusion detection systems and virus filters do monitor their respective domains and take action when a deviation from the rules is detected. People must undertake the role of security enforcement maybe through an information security program. Ogeto (2004) notes that the primary goal of an information security program is to manage risks to information systems. The programs plan is to develop ways to lower current risk through administrative, environmental/ physical and technical measures.

Maroukian (2010) found that the environmental factors which affect a software development team based on a study of five different IT projects in Greek banking sector are IT security policies and standards, software deployment policies and procedures at customer side, rate of software training sessions, rate of formal reviews, walkthroughs, senior management commitment towards both performing organization and customer, system administrators attitude, provisioning of software documentation, project stakeholder ownership.

Clear goals and objectives are essential to guide ongoing organizational efforts for MIS implementation (Cleland and King, 1983). At the outset of MIS implementation projects, it is often very difficult to determine these in a clear manner and lack of clarity results in complexities as the implementation progresses (Slevin and Pinto, 1987).

2.4The Database Exposure and Security of the Management Information System

Managing organizational assets such as data, as well as overall information security concerns, are two of the key technology areas having a large affect on companies today. The enterprise database infrastructure is subject to an overwhelming range of threats. According to the literature (Al-Mashari, 2002; Federici, 2007) another factor that may affect security post implementation of MIS, either positively or negatively, is managing the complexity of information flows (databases). This is much more crucial for companies with branch offices which need to be controlled remotely, leading to a lack of co-ordination (Marshall et al., 2005).

Outdated and duplicated data that is not properly managed during the post implementation of the MIS may also pose a major threat. Arranging, purging and updating organizational data are fundamental processes to ensure the highest level of accuracy possible (Loh and Koh, 2004). Therefore, companies should develop and retain good and disciplined system maintenance processes to ensure quality control of the data stored in their system (Loh and Koh, 2004). It could be argued that if outdated and duplicated data of the system is not discarded properly, it may lead to low data accuracy, erroneous analytical reports and eventually poor decision making at both operational and strategic levels. Additionally, redundant data may reduce speed of data searching and retrieval and increase data storage space and management cost.

Information system security processes and activities provide valuable input into managing IT systems and their development, risk identification, planning and mitigation. A risk management approach involves continually balancing the protection of agency information and assets with the cost of security controls and mitigation strategies throughout the complete information system development life cycle (Saugatuck Technology, 2008).

The enterprise database infrastructure is subject to an overwhelming range of threats. When users (or applications) are granted database access privileges that exceed the requirements of their job function, these privileges may be abused for malicious purpose (Symantec, 2009). A given database user ends up with excessive privileges for the simple reason that database administrators do not have the time to define and update granular access privilege control mechanisms for each user. As a result, all users or large groups of users are granted generic default access privileges that far exceed specific job requirements.

The solution to excessive privileges is query-level access control. Most database software implementations integrate some level of query-level access control (triggers, row-level security, etc), but the manual nature of these "built-in" features make them impractical for all but the most limited deployments. The process of manually defining a query-level access control policy for all users across database rows, columns and operations is simply too time consuming. To make matters worse, as user roles change over time, query policies must be updated to reflect those new roles. Most database administrators would have a hard time defining a useful query policy for a handful of users at a single point in time, much less hundreds of users over time (Infinedo and Nahar, 2007). As a result, most organizations provide users with a generic set of excessive access privileges that work for a large number of users. Automated tools are necessary to make real query-level access control a reality.

According to Lovegrove (2005), users may also abuse legitimate database privileges for unauthorized purposes. Consider a hypothetical rogue healthcare worker with privileges to view individual patient records via a custom Web application. The structure of the Web application normally limits users to viewing an individual patient's healthcare history – multiple records

cannot be viewed simultaneously and electronic copies are not allowed. However, the rogue worker may circumvent these limitations by connecting to the database using an alternative client such as Microsoft Structured Query Language (MS-SQL). Using MS-SQL and his legitimate login credentials, the worker may retrieve and save all patient records. The solution to legitimate privilege abuse is database access control that applies not only to specific queries as described above, but to the context surrounding database access. By enforcing policy for client applications, time of day, location, etc., it's possible to identify users who are using legitimate database access privileges in a suspicious manner.

Attackers may take advantage of database platform software vulnerabilities to convert access privileges from those of an ordinary user to those of an administrator. Vulnerabilities may be found in stored procedures, built-in functions, protocol implementations, and even SQL statements. For example, a software developer at a financial institution might take advantage of a vulnerable function to gain the database administrative privilege. With administrative privilege, the rogue developer may turn off audit mechanisms, create bogus accounts, transfer funds, etc.

Vulnerabilities in underlying operating systems and additional services installed on a database server may lead to unauthorized access, data corruption, or denial of service. In a SQL injection attack, a perpetrator typically inserts (or "injects") unauthorized database statements into a vulnerable SQL data channel. Typically targeted data channels include stored procedures and Web application input parameters. These injected statements are then passed to the database where they are executed. Using SQL injection, attackers may gain unrestricted access to an entire database.

Automated recording of all sensitive and/or unusual database transactions should be part of the foundation underlying any database deployment (Legris and Collerette, 2006). Weak database audit policy represents a serious organizational risk on many levels such as regulatory risk, deterrence and detection and recovery. Database software platforms typically integrate basic audit capabilities but they suffer from multiple weaknesses that limit or preclude deployment.

Denial of Service (DOS) is a general attack category in which access to network applications or data is denied to intended users. Denial of service (DOS) conditions may be created via many techniques - many of which are related to previously mentioned vulnerabilities. For example, DOS may be achieved by taking advantage of a database platform vulnerability to crash a server. Other common DOS techniques include data corruption, network flooding, and server resource overload (memory, CPU, etc.). Resource overload is particularly common in database environments. In addition, weak authentication schemes allow attackers to assume the identity of legitimate database users by stealing or otherwise obtaining login credentials. An attacker may employ any number of strategies to obtain credentials.

2.5The Quality of the Software Application and Security of the Management Information System

In a corporate setting, there are few things more important than setting up a strategy for management of information systems (MIS). The reason is that information systems touch every part of a business operation. Failure to implement any strategy at all is costly. Failure to implement the correct strategy can mean the difference between making a profit and closing the doors. An effective strategy includes several components (Akkermans and van Helden, 2002).

In most cases, systems that are not properly modified to meet new business requirements or are of low quality pose a major threat to the system security. User requirements of the company will constantly change under highly dynamic and competitive market conditions (Ecklundet al., 2006). The implemented MIS should therefore be continuously reviewed and enhanced in the post-implementation phase, in order to meet new user requirements. However, it could be argued that this task may not always be carried out properly in many companies due to low flexibility of the MIS, high reconfiguration cost, lack of in-house experts and insufficient support from system vendors and consultants. If this risk event occurs, the MIS may gradually become less efficient to support user needs, which may significantly impact business operational efficiency and information security.

The information security manager should participate in industry organizations that are actively working on developing metrics and practices that effectively balance business product development needs and risk management (Akkermans and van Helden, 2002). The information security manager should seek training in process management, such as Information Technology Infrastructure Library (ITIL). The information security manager should work closely with line-of business managers to ensure that measurements associated with information security tie to real business risks. Security metrics should tell us about the state or degree of safety relative to a reference point.

System quality reflects the access speed, ease-of-use, navigation and appearance of system application (Kim et al., 2004). Due to the constraints of various terminals and inconvenient input, users may find it difficult to search for information. Thus an interface with powerful navigation, clear layout and prompt responses may be critical to using IS. Poor system quality may lead

users to feel that service providers have not spent enough effort and investment on IS. This will affect their evaluation on the credibility and benevolence of service providers. Vance et al.(2008) reported that system quality including navigational structure and visual appeal affects users' trust in mobile commerce technologies. In addition, system quality may also affect perceived usefulness. Poor system quality causes also include the initial wrong capture of the user specifications, thus creating a system that does not meet the user requirements. Poor system quality will then decrease user expectation of acquiring positive outcomes in future. For example, if users often encounter service interruption or unavailability, they will not be able to conduct ubiquitous payment.

Lack of integration between business and information security is also a major challenge that should be considered in successful implementation of MIS. Senior management should ensure that business liaisons are held accountable for interacting with the information security manager to achieve mutually agreeable risk management objectives. Senior management should ensure that the business strategy is shared with information technology and appropriate risk management groups, such as information security (Amoako-Gyampah, 2004). This will help ensure that necessary adjustments to the information security strategy and technology infrastructure capability can be proactively planned to help manage cost and risk. The information security status associated with high-risk legal and regulatory compliance should be monitored at the executive level to ensure that appropriate priority is given to risk management initiatives.

MIS provide regular information to managers to allow them to make decisions based on data rather than guesses. Certain data and analysis can play a very useful role in making good

decisions about where and when to use human and other resources to achieve the mission of an organization. Managers with quality MIS are able to make decisions from an informed stance rather than a haphazard one.

2.6The After-sales Services of the Vendors and Security of the Management Information System

Maximizing the value derived from IT vendors is key to delivering efficient IT services (Symantec, 2009). Further, the increasing use of outsourcing, out-tasking and cloud computing means that vendors are now playing a fundamental role in IT's delivery of services to the end-user. Given these two factors, effective vendor management has become an essential competency for every IT organization; arguably as important as any internal technology, service management, or program management capability.

In today's competitive marketplace, many companies have moved from a single vendor to a multi-vendor platform (Saugatuck Technology, 2008). Managing the numerous individuals and companies you do business with is crucial for developing valuable relationships. Ensuring that correct vendor information is entered, and updating relevant contracts with new information in a timely manner are two major pain points of vendor management. Vendor Management is a structured approach to receiving the best service and value from a supplier. The core of such a program is the establishment of an ongoing communication channel with a vendor. To improve the vendor management process, it is important to track and evaluate vendors on a regular basis. Not only will regular monitoring of vendors ensure they are meeting your expectations, it will also allow you to proactively take measures to seize opportunities or mitigate risks.

Very often an integrated solution from one single MIS vendor may not satisfy all business needs of the company. Therefore, it is not uncommon for modern companies to procure suitable software modules from different system vendors to form their own unique management information system (Currie, 2003). This approach, however, may increase complexity and difficulty in harmonizing integration issues. In other words, companies may face a risk that seamless integration may not be achieved between current modules or between current and new modules of the MIS. Moreover, Sage (2005), one of the world's leading MIS vendors, reinforces that even if all modules of the MIS are provided by the same vendor, it does not mean they can achieve solid integration. Consequently, this issue may lead to system fragmentation in the company, through the creation of technological islands which are very often totally isolated and non-communicant.

It is important for the vendor's staff to be knowledgeable on both the business process and MIS functions (Stackpole, 2010). Vendors should be carefully selected since vendor support play crucial role in shaping the ultimate outcome of implementation. The project success is found to be positively associated with fit and compatibility with IT vendor employed (Thong et al., 2006).

However, in the context of companies in developing countries, vendors have a very crucial role to play. They should have the agility and flexibility required to implement the requirements of the institutions there with a localised approach. Such a finding also finds support in the study of Yeh and Miozzo (2006). Hence it becomes an added responsibility on the part of vendors to suggest measures to management in bring about a positive organizational climate that is conducive to implementation and also having a localized approach.

2.7The End Users and Security of the Management Information System

The project team competence is another important success factor (Stratman and Roth, 2007). The MIS project involves the entire functional department and demands the efforts and involvement of technical and business experts as well as the end users (Ryan, 2009). As networks grow in size and complexity, the requirement for centralized security policy management tools that can administer security elements is paramount. Sophisticated tools that can specify, manage, and audit the state of security policy through browser-based user interfaces enhance the usability and effectiveness of network security solutions.

Security designing at the system level should take into consideration services obtained externally, planned system interconnections, and the different orientations of system users (e.g., customer service versus system administrators). System users may assist in the development by helping the program manager to determine the need, refine the requirements, and inspect and accept the delivered system. Participants may also include personnel who represent IT, configuration management, design and engineering, and facilities groups. To be successful security, participation is needed from people who are knowledgeable in the disciplines within the system domain (e.g., users, technology experts, operations experts).

Peltier (2005) assert that an effective MIS program cannot be implemented without implementing employee awareness and training program to address policy, procedures and tools. Strong security architecture will be rendered less effective if there is no process in place to make certain that employees are made aware of their rights and responsibilities with regard to organization assets. Employees want to know what is expected of them and who to turn for assistance. Ongoing information security awareness will provide answer to the user community.

Employees need to understand that the security program is supported, approved and directed by the senior management.

Top management support is needed throughout the implementation process (Bingiet al., 2009). The project must align with the strategic business goals. Top management should be the driving force and must be willing for a mindset change by accepting that a lot of learning has to be done at all levels, including themselves (Rao, 2009).One of the factors considered as a major challenge in successful implementation of MIS is lack of senior management's commitment to information security initiatives.

Top manager's attitude "will affect not only the flow of funds and information to the [IS] project, but also the subordinates view the project" (Gargeya and Brady, 2007). Top management support is therefore frequently reported as a crucial factor affecting the success of MIS implementation (Gargeya and Brady, 2005; Loh and Koh, 2007). This factor is certainly also critical to system post-adoption. In truth, lack continuous support from top managers can be a significant risk event that may lead to a set of negative consequences in MIS post-implementation, e.g. conflicts and arguments in MIS issues cannot be solved efficiently, IS development plan is missing or inappropriate, insufficient funds are assigned to system maintenance and enhancement, etc.

Miller et al (2007), supports by observing that senior-level management is often responsible for information security at several levels, including the role as an information owner. Management has a responsibility to demonstrate a strong commitment to an organization's information security program. This commitment can be achieved through corporate information security policy and this policy should include a statement of support from management and should also be signed by the CEO. The management should show leadership by example, a CEO who refuses

to carry a mandatory identification badge or who bypasses system access controls sets a poor example. The management should put in place a compensation scheme for employees where proper security behavior is rewarded accordingly.

Failure of the company to understand information security issues as another major challenge. Information security managers must increase their understanding of the business and their skills in communication through industry-specific education and executive-level continuing education programs. Information security awareness sessions should start at the executive level and hierarchically proceed to the inclusion of all levels of management and employees. Information security managers should seek industry and other publications that target executive and senior management and ensure that those publications are made available to the management team. Senior Management will be in a better position to support security initiatives if they are educated on how critical IT systems are to the continued operation of the enterprise.

High-skilled IT staff are valuable organizational assets, and are crucial for MIS maintenance and enhancement (Ifinedo and Nahar, 2009). However, as widely acknowledged, due to high market demand for this type of professional, companies sometimes may find it difficult to retain their highly qualified MIS experts (Sumner, 2000). This risk event may have a high probability and frequency of occurrence in user companies that have a less efficient retention scheme.

The implemented MIS has to be continuously reviewed and enhanced in the post-adoption stage. A clear IS/IT/ERP development plan is the prerequisite to enable these activities to be carried out successfully. Establishing, implementing and sustaining an efficient IS strategy depends on the commitment of top managers and endeavour of in-house experts. If the IS development plan of the company is missing, ill-defined or is a misfit with the business strategy (Lientz and Larssen,

2006, pp. 124-6), the company will not be able to retain a correct direction for further Enterprise Resource Planning (ERP) development. As a consequence, the implemented MIS system may gradually become incapable to support business strategies and goals.

2.8Conceptual Framework

This part of the research will seek to give clear and consistent definition of the research questions. The conceptual frame work will be used to show the relationship between the dependent variable which is the research problem and the independent variables.

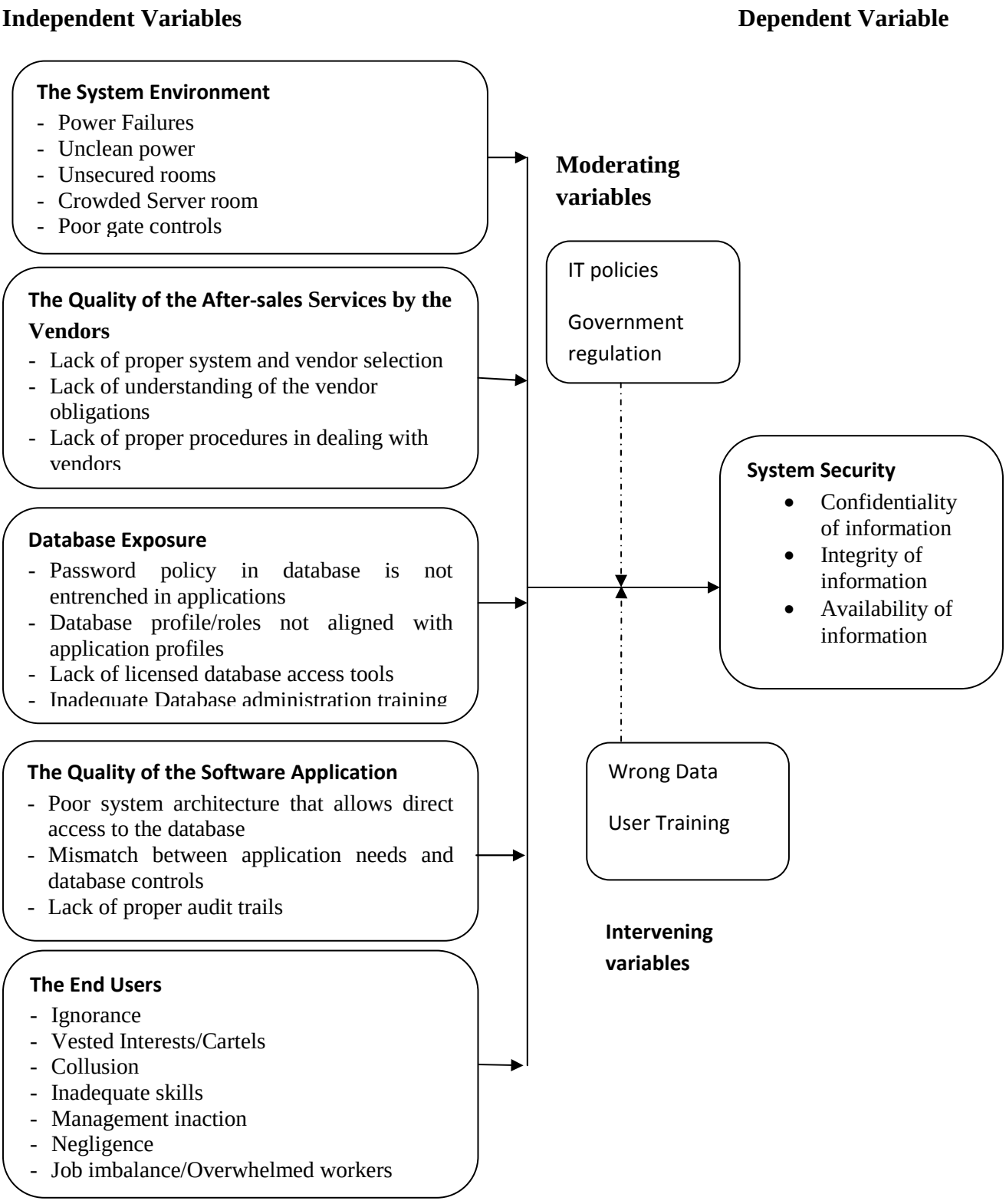

Figure 1: Conceptual Framework

2.9 Chapter Summary

In the last decade, information and information security have moved beyond the boundaries of academia to play key roles to improve overall business objectives and create competitive advantage. More and more businesses around the world now regard information as a vital business asset critical to the success of organizations in today's globally connected and complex business environment. As such, information security is more challenging now than ever before to defend a business against increasingly sophisticated information security threats. Indeed, national and international regulations are calling for organizations to demonstrate due care with respect to security.

CHAPTER THREE

RESEARCH METHODOLOGY

3.1 Introduction

This chapter sets out various stages and phases that will be followed in completing the study. The following subsections are included; research design, target population, sampling design, data collection instruments, data collection procedures and finally data analysis.

3.2 Research Design

The main focus of this study was quantitative. However some qualitative approach was used in order to gain a better understanding and possibly enable a better and more insightful interpretation of the results from the quantitative study. The propose study adopted a case study since it is a research on one organization. A case is an in-depth investigation of an individual, institution or phenomenon (Mugenda and Mugenda, 2003). The primary purpose of a case study was to determine factors and relationships among the factors that have resulted in the behavior under study. Since this study sought to investigate factors affecting system security at NCWSC, a case design is deemed the best design to fulfill the objectives of the study. A case was chosen because it enables the researcher to have an in-depth understanding of the system security at NCWSC.

3.3 Target Population

The target population of this study was the 121 management staff working at NCWSC. The study focused more on the section and particularly on the top and middle level management staff

who are directly dealing with the day to day management of the company since they are the ones conversant with the subject matter of the study. The population characteristic is as summarized in the Table 3.1 below.

Table 3.1: **Target Population**

	Frequency	Percentage
Senior Managers	28	23.2
Middle Level Managers	93	76.8
Total	121	100

Source: HR records as at March, (2012).

3.4 Sample Size and Sampling Procedure

Sample of responding staffs were drawn from 121 top and middle level managers from the staff working at NCWSC. From the population frame the required number of subjects, respondents, elements or firms was selected in order to make a sample. Stratified proportionate random sampling technique was used to select the sample of 30 managers. According to Deming (2007) stratified proportionate random sampling technique produce estimates of overall population parameters with greater precision and ensures a more representative sample is derived from a relatively homogeneous population. The current structure of NCWSC put staff in three categories. From each stratum the study used simple random sampling to select 30 respondents. Statistically, in order for generalization to take place, a sample of at least 30 elements (respondents) must exist (Cooper and Schindler, 2003). The selection was as follows:

Table 3.2: **Sample Size**

	Frequency	Percentage	Sample size
Senior managers (Managers and Directors)	28	0.3	8
Middle level managers (Coordinators and Officers)	93	0.3	22
Total	121		30

3.5 Research Instruments

The study used both primary and secondary data. Primary data was obtained through self-administered questionnaires with closed and open-ended questions and an interview schedule. A 5-point likert scale was used to assess the factors affecting system security at Nairobi City Water and Sewerage Company. The questionnaires included structured and unstructured questions and was administered through drop and pick method to middle level managers. The closed ended questions enabled the researcher to collect quantitative data while open-ended questions enabled the researcher to collect qualitative data. The questionnaire was divided into two sections. Section one is concerned with the general information about respondents, while section two deals with the issues of risk management practices and performance. In addition, an interview guide was used to collect qualitative data from the senior managers. Secondary data was collected by use of desk search techniques from published reports and other documents. Secondary data includes the governments' publications, journals, and periodicals.

3.6 Validity of the Research Instruments

Validity as noted by Robinson (2002) is the degree to which result obtained from the analysis of the data actually represents the phenomenon under study. Validity was via objective questions included in the questionnaire and by pre-testing the instrument to be used to identify and change any ambiguous, awkward, or offensive questions and technique as emphasized by Cooper and Schindler (2003). To establish the validity of the research instrument the researcher sought opinions of experts in the field of study especially the lecturers in the study of information systems and technology.

3.7 Reliability of the Research Instruments

Reliability refers to a measure of the degree to which research instruments yield consistent results (Mugenda and Mugenda, 2003). Reliability of the questionnaire was evaluated through administration of the said instrument to the pilot group of 20 respondents from the target population. The higher the score, the more reliable the generated scale is. A construct composite reliability co-efficient (Cronbach alpha) of 0.7 or above, for all the constructs, was considered adequate for this study. Nunnaly (1978) has indicated 0.7 to be an acceptable reliability coefficient but lower thresholds are sometimes used in the literature.

3.8 Data Collection Procedure

The questionnaires were self administered. Self-administered questionnaires enable one to clarify the questions or probe for more answers. This makes it clear and is likely to yield relevant responses. To increase the response rate, an introduction letter from the University of Nairobi was attached as this assured the respondents of their safety, trust and confidentiality.

3.9 Data Analysis and Presentation

Before processing the responses, the completed questionnaires were edited for completeness and consistency. The data was then be coded to enable the responses to be grouped into various categories. A descriptive analysis was employed in analyzing the quantitative data. Descriptive statistics such as means, standard deviation and frequency distribution will be used to analyze the data. The quantitative data was measured in real values by normalizing. Tables and other graphical presentations as appropriate were used to present the data collected for ease of understanding and analysis. Cooper and Schindler (2003) notes that the use of percentages is important for two reasons; first they simplify data by reducing all the numbers to range between 0 and 100. Second, they translate the data into standard form with a base of 100 for relative comparisons. The qualitative data was coded thematically and then analyzed statistically. Content analysis was used for data that is qualitative nature or aspect of the data collected from the open ended questions and the interview guides.

3.10 Ethical Issues

Ethics as noted by Minja (2009) is referred to, as norms governing human conduct which have a significant impact on human welfare. In this study, confidentiality was of concern in view of the fact that information relevant to the study was of strategic importance to Nairobi City Water and Sewerage Company in Nairobi County. In this regard, the names of the respondents were not disclosed and the names of the information collected the will be held in confidence. Due to sensitivity of some information collected, the researcher holds a moral obligation to treat the information with utmost propriety. Since the respondents might be reluctant to disclose some

information, the researcher needs to reassure the respondents of confidentiality of the information given.

3.11 Operational Definition of Variables

The Operationalization of variables is shown in Table 3.3.

Table 3.3: Operationalization of Variables

Objectives	Variables	Indicators	Scale	Tools of analysis	Type of analysis
To establish how the system environment influences MIS post implementation security	**Independent:** The System Environment	- Power Failures - Unclean power - Unsecured rooms - Crowded Server room - Portability of IT equipment e.g. Laptops, iPods etc. - Poor gate controls - Poor quality of meters - Poor LAN infrastructure - Lack of WAN in some areas	Nominal ordinal	Frequency distribution tables and percentages	Descriptive Content analysis
To establish the extent to which after sale services by the vendor influences MIS post implementation security	The Quality of the After-sales Services by the Vendors	- Lack of proper system and vendor selection - Lack of understanding of the vendor obligations - Lack of proper procedures in dealing with vendors - Lack of Maintenance Contracts and SLAs Non-adherence to contracts with vendors - Vendor locked systems	Nominal ordinal	Frequency distribution tables and percentages	Descriptive
To determine how the database exposure influences MIS post implementation security	Database Exposure	- Password policy in database is not entrenched in applications - Database profile/roles not aligned with application profiles - Lack of licensed database access tools - Inadequate Database administration training - Lack of adequate database management tools	Nominal ordinal	Frequency distribution tables and percentages	Descriptive Content analysis

		- Lack of Disaster Recovery Site and procedures - Lack of backup and recovery procedures - Lack of database access guidelines - Lack of tools to monitor power users in the database - Lack of database patching procedures - Need to maintain numerous passwords			
To assess the influence of the quality of software applications on system security post implementation of management information system	The Quality of the Software Application (MIS)	- Poor system architecture that allows direct access to the database - Mismatch between application needs and database controls - Lack of proper audit trails	Nominal ordinal	Frequency distribution tables and percentages	Descriptive Content analysis Regression
To establish how the end users affect MIS post implementation security	**The End Users**	- Ignorance - Vested Interests/Cartels - Collusion - Inadequate skills - Management inaction - Negligence - Job imbalance/Overwhelmed workers - Lack of succession planning - Non-adherence to leave schedules/policies - Poor induction - Low morale	Nominal ordinal	Frequency distribution tables and percentages	Descriptive Content analysis
	Dependent: System Security	- IT Equipment and Database crashes - Loss of data - Un-authorized access	Nominal ordinal	Frequency distribution tables and percentages	Descriptive Content analysis

		to data and data pilferage - Introduction of viruses and un-authorized software - Ease of tampering with metering data - Difficulties in enforcing system controls - User passwords getting exposed as new passwords are sent through emails. - Long backup and recovery times - Possibility of corrupting database with wrong patches - Un-authentic transactions are introduced e.g. data without source document - Loss of data integrity - System errors/mis-information			

CHAPTER FOUR

DATA ANALYSIS, PRESENTATION AND INTERPRETATIONS

4.1 Introduction

This chapter presents analysis and findings of the study as set out in the research methodology. The study findings and discussions are presented on the factors effecting system security post implementation of management information system at Nairobi City Water and Sewerage Company.

4.1.1 Response Rate

The study targeted a sample of 30 respondents. As Table 4.1 below shows, 24 respondents filled in and returned the questionnaire giving a response rate of 80%. This commendable response rate was made a reality after the researcher made personal visits to remind the respondent to fill-in and return the questionnaires. This response rate was excellent and representative and conforms to Mugenda and Mugenda (2010) stipulation that a response rate of 50% is adequate for analysis and reporting; a rate of 60% is good and a response rate of 70% and over is excellent.

Table 4.1: Response Rate

Response	Frequency	Percent
Responses	24	80
Non-responses	6	20
Total	**30**	**100**

4.2 Demographic Information

4.2.1 Gender of the respondents

The study sought to establish the gender of the respondents. From the findings 4.1 below, 92% of the respondents indicated that they were male while those who indicated that they were female were 8%.

Table 4. 2: Gender of the respondents

	Frequency	Percentage
Male	22	92
Female	2	8
Total	**24**	**100**

4.2.2 Age Bracketof the respondents

The study also sought to determine the age bracket of the respondents. From the findings,30% of the respondents indicated that they were aged between 35-40 years,20% were aged between 25-30 years,15% were aged between 41-44 years,14% were aged between 45-50 years,10% were aged between 31-34 years,6% were aged between 50-60 years while 5% were aged over 51 years.

Table 4. 3: Age Bracket of the respondents

	Frequency	Percentage

31-34	10	2
41-44	15	4
Over 51 years	5	1
25-30 years	20	5
35-40 years	30	7
45-50 years	14	3
50-60 years	6	1
Total	24	100

4.2.3 Highest Education Level

From the findings, 60% of the respondents indicated that they had a postgraduates degree, 35% of the respondents indicated that they had a Bachelors degree while 5% of the respondents indicated that they had a diploma.

Table 4. 4: Highest Education Level

	Frequency	Percentage
Diploma	1	5
Bachelors	8	35
Postgraduate degree	14	60
Total	24	100

4.2.4 Years of Service/Working Period

According to the findings, 88% of the respondents had served for between 1-10 years, 7% of the respondents had served for between 10-20 years while 5% of the respondents had served for between 20-30 years.

Table 4. 5: Years of Service/Working Period

	Frequency	Percentage
1-10 years	21	88
20-30 years	1	5
10-20 years	2	7
Total	24	100

4.3 The System Environment

The report discusses the extent that the system environment affects system security.

4.3.1 System Environment Affect Information System Security in the Company

From the findings, 65% of the respondents indicated that system environment affected information system security in the company to a very great extent, 25% of the respondents indicated that system environment affected information system security in the company to a great extent while 10% of the respondents indicated that system environment affects information system security in the company to a moderate extent.

Table 4. 6:System Environment Affect Information System Security in the Company

	Frequency	Percentage
Very great extent	16	65
Great extent	6	25
Moderate extent	2	10
Total	24	100

4.3.2 Extent do the Following Affect Information System Security in the Company

Table 4.7: Extentdo the Following Affect Information System Security in the Company

	Mean	Std. Deviation
Power Failures	4.7083	0.99909
Unclean power	3.9167	4.26224
Unsecured rooms	4.0417	1.19707
Crowded Server room	3.6789	1.21584
Portability of IT equipment e.g. Laptops, iPods etc.	3.8333	1.57885
Poor gate controls	4.7080	1.23285
Poor quality of meters	4.3333	1.30773
Poor LAN infrastructure	4.7917	1.53167
Lack of WAN in some areas i.e. Sasumua	4.2083	1.31807

From the findings, the respondents indicated that poor LAN infrastructure, power failures and poor gate controls affected information system security in the company to a very great extent as shown by a mean score of 4.7917, 4.7083 and 4.7080 respectively. The respondents also indicated that poor quality of meters, lack of WAN in some areas i.e. Sasumua, unsecured rooms, unclean power and portability of IT equipment e.g. Laptops, iPods etc. affected information

system security in the company to a great extent as shown by a mean score of 4.3333, 4.2083, 4.0417, 3.9167 and 3.8333 respectively.

4.4 The Quality of the After-Sales Services By The Vendors

The report discusses the extent that the quality of the after-sales services by the vendors affect system security.

4.4.1 The Quality of the After-sales Services by the Vendors Affect Information System Security in the Company

According to the findings,75% of the respondents indicated that the quality of the after sales services by the vendors affected information system security in the company to a very great extent,20% of the respondents indicated that the quality of the after sales services by the vendors affected information system security in the company to a great extent while 5% of the respondents indicated that the quality of the after sales services by the vendors affected information system security in the company to a moderate extent.

Table 4.8: The Quality of the After-sales Services by the Vendors Affect Information System Security in the Company

	Frequency	Percentage
Very great extent	75	18
Great extent	20	5
Moderate extent	5	1

Total	100	24

4.4.2 Extent do the Following Affect Information System Security in the Company

Table 4.9:Extent do the Following Affect Information System Security in the Company

	Mean	Std. Deviation
Lack of proper system and vendor selection	3.5450	0.88465
Lack of understanding of the vendor obligations	3.5833	1.01795
Lack of proper procedures in dealing with vendors	3.6258	1.20911
Lack of Maintenance Contracts and SLAs Non-adherence to contracts with vendors	3.7083	0.95458
Vendor locked systems	3.7567	1.32698

According to the findings, the respondents indicated that vendor locked systems, lack of maintenance contracts and SLAs, non-adherence to contracts with vendors, lack of proper procedures in dealing with vendors, lack of understanding of the vendor obligations and lack of proper system and vendor selection affected information system security in the company to a great extent as shown by a mean score of 3.7567, 3.7083, 3.6258, 3.5833 and 3.5450 respectively.

4.5 Database Exposure

The report discusses the extent that database exposure affects system security.

4.5.1 Database Exposure Affect Information System Security in the Company

From the findings, 65% of the respondents indicated that database exposure affected information system security in the company to a very great extent, 25% of the respondents indicated that database exposure affected information system security in the company to a great extent while 10% of the respondents indicated that database exposure affected information system security in the company to a moderate extent.

Table 4. 10: Database Exposure Affect Information System Security in the Company

	Frequency	Percentage
Very great extent	16	65
Great extent	6	25
Moderate extent	2	10
Total	24	100

4.5.2 Extents do the Following Affect Information System Security in the Company

Table 4.11:Extents do the Following Affect Information System Security in the Company

	Mean	Std. Deviation
Password policy in database is not entrenched in applications	3.5667	0.96309
Database profile/roles not aligned with application profiles	3.6333	0.70196
Lack of licensed database access tools	3.7532	1.18872
Inadequate Database administration training	3.9583	0.69025
Lack of adequate database management tools	3.7083	1.08264
Lack of Disaster Recovery Site and Procedures	3.7167	1.34864

According to the findings, the respondents indicated that Inadequate Database administration training, lack of licensed database access tools, lack of disaster recovery site and procedures, lack of adequate database management tools, database profile/roles not aligned with application profiles and password policy in database is not entrenched in applications affected information system security in the company to a great extent as shown by a mean score of 3.9583, 3.7532, 3.7167, 3.7083, 3.6333 and 3.5667 respectively.

4.6 Quality of the Software Application

The report discusses the extent that the quality of the software application affects system security.

4.6.1 Whether the Quality of the Software Application Affect Information System Security in the Company

According to the findings, 75% of the respondents indicated that the quality of the software application affected information system security in the company to a very great extent,20% of the respondents indicated that the quality of the software application affected information system security in the company to a great extent while 5% of the respondents indicated that the quality

of the software application affected information system security in the company to a moderate extent.

Table 4. 12: Whether the Quality of the Software Application Affects Information System Security in the Company

	Frequency	Percentage
Very great extent	18	75
Great extent	5	20
Moderate extent	1	5
Total	24	100

4.6.2 Extent do the Following Affect Information System Security in the Company

Table 4.13: Extent do the Following Affect Information System Security in the Company

	Mean	**Std. Deviation**
Poor system architecture that allows direct access to the database	4.5373	.65893
Lack of integrity of staff	3.9552	1.17335
Mismatch between application needs and database controls	3.9104	1.01102

Lack of proper audit trails	4.0597	.71522

From the findings, the respondents indicated that poor system architecture that allowed direct access to the database affected information system security in the company to a very great extent as shown by a mean score of 4.5373, the respondents indicated that lack of proper audit trails, lack of integrity of staff and mismatch between application needs and database controls affected information system security in the company to a great extent as shown by a mean score of 4.0597, 3.9552 and 3.9104 respectively.

4.7 The End User

The report discusses the extent that the end users affect system security.

4.7.1 Extent does the End Users Affect Information System Security in the Company

According to the findings, 70% of the respondents indicated that end user effect affected information system security in the company to a very great extent, 20% of the respondents indicated that end user effect affected information system security in the company to a great extent while 10% of the respondents indicated that end user effect affected information system security in the company to a moderate extent.

Table 4. 14: Extent does the End Users Affect Information System Security in the Company

	Frequency	Percentage
Very great extent	17	70

Great extent	5	20
Moderate extent	2	10
Total	24	100

4.7.2 Extent do the following affect Information System Security in the Company

Table 4. 15: Extent do the following affect Information System Security in the Company

	Mean	Std. Deviation
Ignorance	4.6716	.56106
Vested Interests/Cartels	4.5373	.63552
Collusion	4.4925	.68253
Management inaction	4.5166	.49875
Negligence	4.6269	.51745
Job imbalance/Overwhelmed workers	4.6418	.59548
Lack of succession planning	3.9254	.85835
Non-adherence to leave schedules/policies	4.4908	.86225
Poor induction	3.8718	.79898
Low morale	4.1941	.96770

From the findings, the respondents indicated that ignorance, job imbalance/overwhelmed workers, negligence , vested Interests/Cartels and management inaction affected information system security in the company to a great extent as shown by a mean score of 4.6716, 4.6418,4.6269, 4.5373, 4.5166,respectively.The respondents indicated that collusion, non-

adherence to leave schedules/policies, low morale, lack of succession planning and poor induction affected information system security in the company to a great extent as shown by a mean score of 4.4925, 4.4908, 4.1941, 3.9254 and 3.8718 respectively.

4.8 System Security

4.8.1 Trend of the Following Aspects of System Security Post Implementation of Management Information System

Table 4.16: Trend of the following aspects of System Security Post Implementation of Management Information System

	Mean	Std. Deviation
IT Equipment and Database crashes	4.0808	1.03684
Loss of data	4.4242	5.24908
Un-authorized access to data and data pilferage	3.8687	1.10330
Introduction of viruses and un-authorized software	4.2727	.90145
Ease of tampering with metering data	4.0303	1.20070
Difficulties in enforcing system controls	3.9495	1.04368
User passwords getting exposed as new passwords are sent through emails.	4.1414	.94772
Long backup and recovery times	3.9394	1.03823
Possibility of corrupting database with wrong patches	4.4747	.76055
Un-authentic transactions are introduced e.g. data without source document	4.3232	1.00842

Loss of data integrity	2.9192	1.43340
System errors/ mis-information	2.6162	1.46181

From the findings, the respondents indicated that possibility of corrupting database with wrong patches, loss of data, un-authentic transactions are introduced e.g. data without source document, introduction of viruses and un-authorized software, user passwords getting exposed as new passwords are sent through emails, IT Equipment and Database crashes, ease of tampering with metering data , difficulties in enforcing system controls, long backup and recovery times and un-authorized access to data and data pilferage had improved as shown by a mean score of 4.4747, 4.4242, 4.3232, 4.2727, 4.1414, 4.0808,4.0303, 3.9495, 3.9394 and 3.8687 respectively. The respondents indicated that loss of data integrity and system errors/ mis-information remained constant as shown by a mean score of 2.9192 and 2.6162 respectively.

CHAPTER FIVE

SUMMARY OF FINDINGS, DISCUSSION, CONCLUSIONS AND RECOMMENDATIONS

5.1 Introduction

This chapter presented the discussion of key data findings, conclusion drawn from the findings highlighted and recommendation made there-to. The conclusions and recommendations drawn were focused on addressing the objective of the study.

5.2 Summary of Findings

The study sought to establish the factors effecting system security post implementation of management information system at NCWSC.

5.2.1 The System Environment

The study deduced that poor LAN infrastructure, power failures and poor gate controls affected information system security in the company to a very great extent .The study also deduced that poor quality of meters, lack of WAN in some areas i.e. Sasumua, unsecured rooms, unclean power and portability of IT equipment e.g. Laptops, iPods etc. affected information system security in the company to a great extent.

5.2.2 The Quality of the After-Sales Services by the Vendors

The study further established that vendor locked systems, lack of maintenance contracts and SLAs non-adherence to contracts with vendors, lack of proper procedures in dealing with vendors, lack of understanding of the vendor obligations and lack of proper system and vendor selection affected information system security in the company to a great extent.

5.2.3 Database Exposure

The study established that inadequate database administration training, lack of licensed database access tools, lack of disaster recovery site and procedures, lack of adequate database management tools, database profile/roles not aligned with application profiles and password policy in database is not entrenched in applications affected information system security in the company to a great extent.

5.2.4 Quality of the Software Application

This study also revealed that poor system architecture that allowed direct access to the database affected information system security in the company to a very great extent. The study also established that lack of proper audit trails, lack of integrity of staff and mismatch between application needs and database controls affected information system security in the company to a great extent.

5.2.5 The End User

This study also established that ignorance, job imbalance/overwhelmed workers, negligence, vested Interests/Cartels and management inaction affected information system security in the company to a great extent. The study further deduced that collusion, non-adherence to leave schedules/policies, low morale, lack of succession planning and poor induction affected information system security in the company to a great extent.

5.2.6 System Security

This study revealed that possibility of corrupting database with wrong patches, loss of data, un-authentic transactions are introduced e.g. data without source document, introduction of viruses and un-authorized software, user passwords getting exposed as new passwords are sent through emails, IT Equipment and Database crashes, ease of tampering with metering data , difficulties in enforcing system controls, long backup and recovery times and un-authorized access to data and data pilferage had improved.

5.3 Discussion

This section sought to discuss the factors effecting system security post implementation of management information system at NCWSC in the light of previous studies done.

5.3.1 Systems Environment

The study deduced that poor LAN infrastructure, power failures and poor gate controls affected information system security in the company. This agrees with Cohen and Bailey (2008), environmental factors, design factors, employees' psychological traits and internal and external processes can predict the MIS effectiveness. The turnover in the industry, at the managerial level, can also affect the performance of software development teams in the organization. The study also deduced that poor quality of meters, lack of WAN in some areas i.e. Sasumua, unsecured rooms, unclean power and portability of IT equipment e.g. Laptops, iPods etc. affected information system security in the company. This concurs with Ebert and Neve (2001) who stated that work environment and effective and efficient tools are some of the glues for

global software development projects. The distribution of software development globally results into multicultural engineers work together results into innovative products and processes.

5.3.2 The Quality of the After-Sales Services by the Vendors

The study further established that vendor locked systems, lack of maintenance contracts and SLAs non-adherence to contracts with vendors, lack of proper procedures in dealing with vendors, lack of understanding of the vendor obligations and lack of proper system and vendor selection affected information system security in the company. This is in line with Akkermans and Van Helden (2002), who argue that in a corporate setting, there are few things more important than setting up a strategy for management of information systems (MIS). The reason is that information systems touch every part of a business operation. Failure to implement any strategy at all is costly. Failure to implement the correct strategy of handling contracts can mean the difference between making a profit and closing the doors.

5.3.3 Database Exposure

The study established that Inadequate Database administration training, lack of licensed database access tools, lack of disaster recovery site and procedures, lack of adequate database management tools, database profile/roles not aligned with application profiles and password policy in database is not entrenched in applications affected information system security in the company. This concurs with Al-Mashari (2002), who explains that managing organizational assets such as data, as well as overall information security concerns, are two of the key technology areas having a large affect on companies today. The enterprise database infrastructure is subject to an overwhelming range of threats. Another factor that may affect

security post implementation of MIS, either positively or negatively, is managing the complexity of information flows (databases). This is much more crucial for companies with branch offices which need to be controlled remotely, leading to a lack of co-ordination.

5.3.4 Quality of the Software Application

This study also revealed that poor system architecture that allowed direct access to the database affected information system security in the company. This is in line with Ecklundet al., (2006) who explains that in most cases, systems that are not properly modified to meet new business requirements or are of low quality pose a major threat to the system security. User requirements of the company will constantly change under highly dynamic and competitive market conditions. The implemented MIS should therefore be continuously reviewed and enhanced in the post-implementation phase, in order to meet new user requirements. However, it could be argued that this task may not always be carried out properly in many companies due to low flexibility of the MIS, high reconfiguration cost, lack of in-house experts and insufficient support from system vendors and consultants. If this risk event occurs, the MIS may gradually become less efficient to support user needs, which may significantly impact business operational efficiency and information security.

The study also established that lack of proper audit trails, lack of integrity of staff and mismatch between application needs and database controls affected information system security in the company. Vance et al. (2008) reported that system quality including navigational structure and visual appeal affects users' trust in mobile commerce technologies. In addition, system quality may also affect perceived usefulness.

5.3.5 The End User

The study further deduced that collusion, non-adherence to leave schedules/policies, low morale, lack of succession planning and poor induction affected information system security in the company .This is in line with Ryan (2009) who explains that the MIS project involves the entire functional department and demands the efforts and involvement of technical and business experts as well as the end users. As networks grow in size and complexity, the requirement for centralized security policy management tools that can administer security elements is paramount. Sophisticated tools that can specify, manage, and audit the state of security policy through browser-based user interfaces enhance the usability and effectiveness of network security solutions.

5.4 Conclusions

The researcher concluded that environmental factors, design factors, employees' psychological traits and internal and external processes can predict the MIS effectiveness.

The researcher also concludes that arranging, purging and updating organisational data are fundamental processes to ensure the highest level of accuracy possible. Information system security processes and activities provide valuable input into managing IT systems and their development, risk identification, planning and mitigation. A risk management approach can be employed to continually balance the protection of NCWSC's information and assets with the cost of security controls and mitigation strategies throughout the complete information system development life cycle.

The researcher also concludes that during the selection of systems, it is critical to ensure that user requirements are obtained to ensure that the system purchased meets the strategic goals of the organization and will fulfill the needs of the employees.

The researcher further concludes that as networks grow in size and complexity, the requirement for a centralized security policy management tool that can administer security elements in NCWSC is paramount.

5.5 Recommendations

The researcher recommends that:

1. Companies should develop and retain good and disciplined system maintenance processes to ensure quality control of the data stored in their system

2. Since vendors have a very crucial role to play, the researcher recommends that they should have the agility and flexibility required to implement the requirements of the institutions there with a localized approach.

3. Security designing at the system level should take into consideration services obtained externally, planned system interconnections, and the different orientations of system users (e.g., customer service versus system administrators).

4. The system end users (employees) may assist in the development by helping to determine the needs i.e. giving their requirements for the system, refine the requirements, and inspect and accept the delivered system.

5. To be a successful system implementation, participation is needed from people who are knowledgeable in the disciplines within the system domain e.g. quality assurance services from audit firms such as PwC, KPMG who ensure that system implementation was done correctly and the user requirements met.

6. An information system security policy should be developed and communicated throughout the organization.

5.6 Suggestion for Further Studies

Another study should be done to investigate if there are any other challenges that may face system security at NCWSC considering the company is in the process of implementing an ERP system. A similar study should also be done on other water service providers in the country to allow for generalization. Further studies should be done on the uptake, dissemination and impact of information security policies within organizations.

REFERENCES

Akkermans, H., van Helden, K. (2002). Vicious and virtuous cycles in ERP implementation: a case study of interrelations between critical success factors, *European Journal of Information Systems*, Vol. 11 pp.35.

Amoako-Gyampah, K. (2004). ERP implementation factors a comparison of managerial and end-user perspectives, *Business Process Management Journal*, Vol. 10 pp.171.

Andersen, B. (2001). *Governing for Enterprise Security*, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA, available at: www.sei.cmu.edu/reports/05tn023.pdf

Azah A. N. and Norizan M. Y. (2010). An Analysis of Information Systems Security Management (ISSM): The Hierarchical Organizations vs. Emergent Organization. *International Journal of Digital Society (IJDS).* Volume 1, Issue 3.

Bajwa, D.S., Garcia, J.E., Mooney, T. (2004). An integrative framework for the assimilation of enterprise resource planning systems: phases, antecedents, and outcomes, *Journal of Computer Information Systems*, Vol. 44 pp.81-90.

Bee, R. and Bee, F.,(2009). *Managing Information and Statistic*. Trowbridge: Cromwell Press.

Bosworth, N., West, S. G., & Aiken, L. S. (2002). Using the balanced scorecard as a strategic management system, *Harvard Business Review*, Vol. 85 No.7/8, pp.150-61.

Bradley, J. and Lee, C.C. (2004). *ERP training and user satisfaction*, paper presented at the 10th Americas Conference on Information Systems, New York, NY, .

Calder, N. (2005). *Risk Management and Analysis*. In Tipton, H. F. (Eds). Information Security Management Handbook (pp.751). Boca Raton, FL, USA: Auerbach Publishers, Incorporated.

Cohen, S.G., Bailey, D.E. (2008). What makes teams work: group effectiveness research from the shop floor to the executive suite, *Journal of Management*, Vol. 23 No.3, pp.239-90.

Cooper, D., & Schinder, P. (2003). Business Research methods (8th Ed.). new delhi: tata mcgraw hill.

Dhillon, G. and Backhouse, J. (2001). Current directions in IS security research: towards socio-organizational perspectives. *Information Systems Journal*,11(2):127-153.

Ebert, C., Neve, P.D. (2001). *Surviving global software development*, IEEE Software, No.March/April, pp.62-69.

Eisenhardt, M, K. (2009). Agency theory: An assessment and review. *Academy of Management Review,* 14(1). 57).

Ernst and Young (2008). *Ernst and Young 2008's global information security survey*, available at: www.ey.com/Publication/vwLUAssets/GISS_2008/$FILE/GISS2008.pdf (accessed 28 October 2010). .

Federici, T. (2007). *Information systems outsourcing*: A survey and analysis of the literature.The DATA BASE for Advances in Information Systems , 35(4):6-102.

Freeman, R.E. (1984). *Strategic Management*: A Stakeholder Approach, Pittman, Boston, MA, .

Furnell, V. and Warren, T. (2009). Information Security Management A New Paradigm. In Proceedings of SAICSIT,130-136.

Garg, D., Friedman, M. and Savage, L. (2003). The impact of culture on the adoption of it: an interpretive study. *Journal of Global Information Management*, 7(1):5-15.

Gargeya, C. and Brady, E. (2007). Information security policy - what do international information security standards say? *Computers & Security* , 21(5):402-409.

Gichuru, D. C. (2000).*An investigation of computer security status at the University of Nairobi*.MSc | University of Nairobi, Kenya.

Hawaii International Conference on System Sciences, Proceedings of the 41st Annual , pages 454-454.

Infinedo, P. and Nahar, N. (2007). ERP systems success: an empirical analysis of how two organizational stakeholder groups prioritize and evaluate relevant measures, *Enterprise Information Systems*, Vol. 1 pp.24-48.

ISO (2003). Information technology — Security techniques — Code of practice for information security management Information Technology Governance Institute (2006). The international standards ISO/IEC.

Kairab, B. (2005). Analyzing information systems development: A comparison and analysis of eight is development. *Information Systems Journal*, 21(7):551-575.

Knight, J., (2009).*Computing for Business*. Essex: Pearson Education Ltd.

Kossek, E.E. (2007). The acceptance of human resource innovation by multiple constituencies, *Personnel Psychology*, Vol. 42 pp.263-81.

Laudon, K., andLaudon, J. (2010). *Management information systems*: Managing the digital firm. (11th ed.). Upper Saddle River, NJ: Pearson Prentice Hall.

Layton, T. P. (2007). *Information Security: Design, Implementation, Measurement, and Compliance.* Boca Raton, FL: Auerbach publications. ISBN 978-0-8493-7087-8.

Legris, P., Collerette, P. (2006). A roadmap for IT project implementation: integrating stakeholders and change management issues, *Project Management Journal*, Vol. 37 pp.64-75.

Lientz, B. and Larssen, J. (2006). Information security: management's effect on culture and policy. *Information Management &Computer Security*, 14(1):24-36.

Loh, S. and Koh, G. (2004). Barriers to e-government integration. *Journal of Enterprise Information Management* , 18(5/6):511-530.

Maroukian, K. (2010). IT project environment factors affecting requirements analysis in service provisioning for the Greek banking sector, *Journal of Software Engineering and Applications,* Vol. 3 pp.858-68.

McCumber T. (2005). *Introduction to information systems*.13th ed. McGraw-Hill/Irwin, New York.

Miller, M., Ramamurthy, K., and Saunders, C. S. (2007). Information processing view of organizations: An exploratory examination of fit in the context of inter-organizational relationships. *Journal of Management Information Systems*, 22,1, 257-294

Minja, O. (2009). Qualitative Research in Information Systems. *Journal of the Academy of Marketing Science* , 29(3):255-275.

Moule, B. and Giavara, D. (2009).). Dierent perspectives on information systems: Problems and solutions. *ACM Computing Surveys* , 19(1).

Mugenda, M., O., & Mugenda, G., A. (2003). *Research Methods.* Nairobi: Acts Press.

Norman, A.A. and Yasin, N.M. (2010). *An analysis of Information Systems Security Management (ISSM):* The hierarchical organizations vs. emergent organization. Fac. of Comput.Sci.and Inf. Technol., Univ. of Malaya, Kuala Lumpur, London.

Nunnaly, P. (1978). *Practical Research: planning and design.* New York: Macmillan.

Obara M. P. (2010). Information systems implementation In state corporations.A Critical Evaluation of the Process and Challenges in Kenyan Parastatals.*AIBUMA PublishingAfrican Journal of Business and Management (AJBUMA).* Vol. 1 (2010). 23 pages Science, School of Business- University of Nairobi

Osborne, R. (2006). Information technology and organizational change: causal structure in theory and research. *Management Science*, 34(5):583-599.

Peltier, B. (2005). *Information security culture*. In: IFIP TC11 international conference on information security , Cairo, Egypt, pages 7-9.

Rajendra S. and Ajay M. (2011).An Investigation of the Factors Affecting the Security of Management Information System in Financial Institutions.*The IUP Journal of Systems Management.*Article IJSyM11105.**P** : 21

Robinson, S. (2002). *Research Methods in the social sciences.* London: Arnold.

Ross, B. (2007). Evaluating public sector information systems: More than meets the eye. *Public Administration Review*. 51(5):377-384.

Ryan, S. (2009). Information security cultures of four professions: A comparative study.

Sage, P. (2005). Public sector information system critical success factors. Transforming Government: People, Process and Policy , 2(1):60-70.

Saugatuck Technology (2008). *Enterprise information management for competitive advantage,* available at: www.synaptica.com/djcs/synaptica/Enterprise%20Information%20Mgmt_DJWhitepaper033108.pdf (accessed 28 October 2010). .

Schein, E.H. (2006). *The Role of the CEO in the Management of Change*: The Case of Information Technology, MIT Press, Cambridge, MA, .

Siponen, W, (2000). *Analyzing information security culture*: increased trust by an appropriate information security culture. Database and Expert Systems Applications, Proceedings. 14th International Workshop, pages 405-409.

Sookdawoor, G. (2005). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security* , 8(1):3141.

Stackpole, A. (2010). Information Security Management Best Practice Based on ISO/IEC 17799. *Information Management Journal* , 39(4):60-66.

Symantec, T. (2009). *Symantec internet security threat report trends for 2008*, available at: http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiv_04-2009.en-us.pdf.

Ward, J. and Peppard, J. (2010). Mind the gap: diagnosing the relationship between the IT organization and the rest of business, *Journal of Strategic Information Systems,* Vol. 8 pp.29-60.

Wider, D. and Davis, H. (2008). *Critical analysis of different approaches to minimizing user-related faults in information systems security*: implications for research and practice. Information Management & Computer Security , 8(5):197-209.

Wylder, N. (2004). A review of information security issues and respective research contributions. *SIGMIS Database*, 38(1):60-80.

Yeh, B. and Miozzo, R. (2006). Towards information security behavioral compliance. *Computers & Security* , 23(3):191-198.

APPENDICES

Appendix I: Introduction Letter

Gladys Wambui Njoroge

P.O. Box 39321 - 00623

Nairobi

July 21st, 2012

Dear Sir/Madam,

RE: REQUEST FOR PARTICIPATION IN A RESEARCH STUDY

I am a final Masters of Arts degree student at the University of Nairobi. My area of specialization is project planning and management. I am currently undertaking a research on "**Factors Influencing Management Information System Post Implementation System Security: A Case Study Of Nairobi City Water And Sewerage Company, Kenya**".

I would be grateful if you could spare some time from your busy schedule and complete the enclosed questionnaire. All the information provided will be used purely for academic purposes only and will be treated with utmost confidentiality.

Thank you for your cooperation.

Yours faithfully,

Gladys Wambui Njoroge

L50/60567/2010

Appendix I1: Research Questionnaire for Middle and Low level Managers

Instructions: Please tick in the appropriate bracket or provided spaces

SECTION A: BIO DATA

1. Gender: Male [ ] Female [ ]

2. Your age bracket (Tick whichever appropriate)

18 - 24 Years	[ ]	25 - 30 Years	[ ]
31 - 34 years	[ ]	35 - 40 years	[ ]
41 - 44 years	[ ]	45 - 50 years	[ ]
Over- 51 years	[ ]	50 - 60 years	[ ]

3. What is your highest education level? (Tick as applicable)

Primary	[ ]	Secondary	[ ]
Diploma/certificate	[ ]	Bachelors' degree	[ ]
Postgraduate degree	[ ]	Others-specify……	

4. Years of service/working period (Tick as applicable)

1-10 years	[ ]	10-20 years	[ ]
20-30 years	[ ]	Over 30 years	[ ]

Section B: factors influencing management information system post implementation system security

THE SYSTEM ENVIRONMENT

1) To what extent does the system environment affect information system security in your company?

   Very great extent [ ] Great extent [ ]

   Moderate extent [ ] Little extent [ ]

   Not at all [ ]

2) To what extent do the following affect information system security in your company?

	Very great extent	**Great extent**	**Moderate extent**	**Little extent**	**Not at all**
Power Failures					
Unclean power					
Unsecured rooms					
Crowded Server room					
Portability of IT equipment e.g. Laptops, iPods etc.					
Poor gate controls					
Poor quality of meters					
Poor LAN infrastructure					
Lack of WAN in some areas i.e. Sasumua					

THE QUALITY OF THE AFTER-SALES SERVICES BY THE VENDORS

3) To what extent does The Quality of the After-sales Services by the Vendors affect information system security in your company?

Very great extent [ ] Great extent [ ]

Moderate extent [ ] Little extent [ ]

Not at all [ ]

4) To what extent do the following affect information system security in your company?

	Very great extent	Great extent	Moderate extent	Little extent	Not at all
Lack of proper system and vendor selection					
Lack of understanding of the vendor obligations					
Lack of proper procedures in dealing with vendors					
Lack of Maintenance Contracts and SLAs Non-adherence to contracts with vendors					
Vendor locked systems					

DATABASE EXPOSURE

5) To what extent does Database Exposure affect information system security in your company?

Very great extent [ ] Great extent [ ]

Moderate extent [ ] Little extent [ ]

Not at all [ ]

6) To what extent do the following affect information system security in your company?

	Very great extent	Great extent	Moderate extent	Little extent	Not at all
Password policy in database is not entrenched in applications					
Database profile/roles not aligned with application profiles					
Lack of licensed database access tools					
Inadequate Database administration training					
Lack of adequate database management tools					
Lack of Disaster Recovery Site and procedures					
Lack of backup and recovery procedures					
Lack of database access guidelines					
Lack of tools to monitor power users in the database					
Lack of database patching procedures					
Need to maintain numerous passwords					

7) To what extent doesthe quality of the software application (MIS) affect information system security in your company?

Very great extent [ ] Great extent [ ]

Moderate extent [ ] Little extent [ ]

Not at all [ ]

8) To what extent do the following affect information system security in your company?

	Very great extent	**Great extent**	**Moderate extent**	**Little extent**	**Not at all**
Poor system architecture that allows direct access to the database					
Lack of integrity of staff					
Mismatch between application needs and database controls					
Lack of proper audit trails					

THE END USERS

9) To what extent dothe end users affectinformation system security in your company?

Very great extent [ ] Great extent [ ]

Moderate extent [ ] Little extent [ ]

Not at all [ ]

10) To what extent do the following affect information system security in your company?

	Very great extent	**Great extent**	**Moderate extent**	**Little extent**	**Not at all**
Ignorance					
Vested Interests/Cartels					
Collusion					
Inadequate skills					
Management inaction					
Negligence					
Job imbalance/Overwhelmed workers					
Lack of succession planning					

Non-adherence to leave schedules/policies					
Poor induction					
Low morale					

SYSTEM SECURITY

11) What is the trend of the following aspects of system security post implementation of management information system at Nairobi City Water and Sewerage Company for the last five years?

	Greatly Improved	Improved	Constant	Decreasing	Greatly decreased
IT Equipment and Database crashes					
Loss of data					
Un-authorized access to data and data pilferage					
Introduction of viruses and un-authorized software					
Ease of tampering with metering data					
Difficulties in enforcing					

system controls					
User passwords getting exposed as new passwords are sent through emails.					
Long backup and recovery times					
Possibility of corrupting database with wrong patches					
Un-authentic transactions are introduced e.g. data without source document					
Loss of data integrity					
System errors/ mis-information					

THANK YOU

Appendix III: Interview Guide for Top level managers

1) Kindly describe the general level of information system security in your company?

2) What are some of the operational environment issues that affect information security in your company?

3) How does the system environment influence system security post implementation of management information system?

4) What are some of the after sale services offered by the vendor? How would you rate them?

5) How does after sale services by the vendor influence system security post implementation of management information system?

6) How does the database exposure influence system security post implementation of management information system?

7) Briefly describe the quality of the software applications in your company

8) In what ways does quality of the software applications affect system security post implementation of management information system?

9) What are some of the ways in which the end users influence system security post implementation of management information system?

10) What are some of the suggestions on how to increase system security post implementation of management information system?