

**FACTORS INFLUENCING THE LEVEL OF INFORMATION SECURITY
PRACTICE IN STATE CORPORATIONS: A CASE OF MINISTRY OF
INDUSTRIALIZATION, KENYA**

BY:

OKOTH WASHINGTON ODUOR

**UNIVERSITY OF NAIROBI
KIKUYU LIBRARY
P. O. Box 92
KIKUYU**

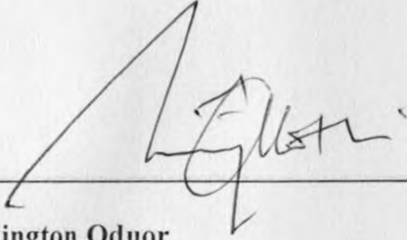
**A RESEARCH PROJECT REPORT SUBMITTED IN PARTIAL FULFILMENT AS
A REQUIREMENT FOR THE AWARD OF THE DEGREE OF
MASTER OF ARTS IN
PROJECT PLANNING AND MANAGEMENT,
OF THE UNIVERSITY OF NAIROBI.**

2012

DECLARATION

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

Signature: _____



Okoth Washington Oduor

REG. NO. L50/76906/2009

Date: _____

31/7/12

This research project has been submitted for Examination with my approval as University Supervisors.

Signature: _____



Dr. Christopher Mwangi Gakuu

Senior Lecturer, Department of Extra Mural Studies,

University of Nairobi

Date: _____

31/7/2012

DEDICATION

I dedicate this work to my wife Ombette Scholastica and our sons Tonny, Jerry, Lloyd and Ian for their encouragement. To my sons, thanks a lot for checking on my course work performance as I also checked your school assignments.

ACKNOWLEDGEMENT

I am indebted to my supervisors, Dr. Christopher Mwangi Gakuu for his moral support and encouragement. He was flexible to allow me send my drafts by email and was always available whenever I needed help.

Special thanks go to my family for the moral support and assisting in typing this draft and making numerous spelling and grammatical corrections resulting from my pressure of work. I could not get a better secretary.

I acknowledge the support accorded to me by my employer Kenya Bureau of Standards, the PS Ministry of Industrialization, Prof. Kibicho Karanja and all my colleagues in the ICT industry.

I also acknowledge the encouragement from my friends, sisters and brothers. I also thank Samuel Onjolo and Samuel Ronoh for their constant prayers. Last but not least, I acknowledge the contribution of my fellow students, the M.A. in Project Planning and Management class of 2009 who demonstrated seriousness and a sincere desire to learn by *freely sharing and contributing to class discussions* hence enriching the content of any single topic. To you all, I say, may God bless you.

LIST OF ABBREVIATIONS AND ACRONYMS

IS	Information Security
CIA	Confidentiality Integrity & Availability
CIO	Chief Information Officer
GDP	Gross Domestic Product
GSISS	Global State of Information Security Survey
ISO	International Organization for Standardization
ICT	Information and Communication Technology
IDs	Identifications
IEC	International Electrotechnical Commission
CERT	Computer Emergency Response Team
NIST	National Institute of Standards and Technology
DRP	Disaster Recovery Plan
KEBS	Kenya Bureau of Standards
ISMS	Information Security Management System
QMS	Quality Management System
DISC	International Symposium on Distributed Computing
DOD	Department of Defence

MV	Moderating Variable
PV	Predictor Variable
IV	Intervening Variable
DV	Dependent Variable
EV	Extraneous Variable
ISP	Information Security Practice

LIST OF TABLES

Table 3.1: Sampling Frame.....	Page 27
Table 3.2: Operational Definitions of Variables.....	Page 31
Table 4.1: Organization of the respondent.....	Page 36
Table 4.2: Position of the respondent.....	Page 37
Table 4.3: Age bracket of the respondent	Page 38
Table 4.4: Information security role of the respondent	Page 38
Table 4.5: Presence of access control	Page 39
Table 4.6: Access control mechanisms	Page 39
Table 4.7: Human factor determinants	Page 41
Table 4.8: Mechanisms to ensure competence of security team members.	Page 41
Table 4.9: Information security management tools	Page 42
Table 4.10: Information security technology measures	Page 43
Table 4.11: Frequency of usage	Page 43
Table 4.12: Managing information security	Page 45
Table 4.13: Managing intrusion to organization data/information.....	Page 45
Table 4.14: Preventing organization network from public network	Page 46
Table 4.15: Data Risk Management	Page 47
Table 4.16: Incident Response and Management	Page 48
Table 4.17: Frequency of information security awareness	Page 49
Table 4.18: Presence of internal policies and procedures	Page 50
Table 4.19: Information security enforcement and assessment	Page 50
Table 4.20: Level of information security practice	Page 51
Table 4.21: Conformity to regulatory requirements	Page 52
Table 4.22: Satisfaction with research objectives	Page 52

UNIVERSITY OF NAIROBI
KIKUYU LIBRARY
P. O. Box 92
KIKUYU

LIST OF FIGURES

Figure 1 Conceptual Framework Page 25

TABLE OF CONTENT

DECLARATION	ii
DEDICATION	iii
ACKNOWLEDGMENT	iv
LIST OF ABBREVIATIONS AND ACRONYMS	v
LIST OF FIGURES AND TABLES	vii
ABSTRACT	1
CHAPTER ONE: INTRODUCTION	2
1.1 Background of the Study.....	2
1.2 Statement of Problem.....	5
1.3 Purpose of the Study	6
1.4 Objectives of the Study	6
1.5 Research Questions.....	7
1.6 Significance of the Study	7
1.7 Delimitations of the Study	8
1.8 Limitation of the Study	9
1.9 Basic Assumptions of the Study.....	9
1.10 Definition of Significant terms used.....	10
1.11 Organization of the Study	11
CHAPTER TWO: LITERATURE REVIEW	12
2.1 Introduction	12
2.2 Concept of Information Security	12
2.3 Information Security Practice.....	14
2.4 Access Control Mechanisms	15
2.5 Information Systems Management Tools Usage.....	16
2.6 Information Systems Technology Usage	19
2.7 Human Factors in Information Security Practice.....	20
2.8 Security Infrastructure.	22
2.9 Conceptual Framework	25
CHAPTER THREE: RESEARCH METHODOLOGY	26
3.1 Introduction	26

3.2	Research Design	26
3.3	Target Population	26
3.4	Sampling Procedure and Sample Size	27
3.5	Methods of Data Collection	28
3.6	Validity and Reliability	29
3.7	Operational Definition of Variables	31
3.8	Methods of Data Analysis	35
3.9	Summary of Chapter	35
 CHAPTER FOUR: DATA ANALYSIS, PRESENTATION AND INTERPRETATION ..		36
4.1	Introduction	36
4.2	Background Characteristics of Respondents.....	36
4.3	Access Control.....	39
4.4	Human Factors.....	41
4.5	Information Systems Management Tools Usage.....	43
4.6	Information Systems Technology Usage	43
4.7	Security Infrastructure.	48
4.8	Summary.	55
 CHAPTER FIVE: SUMMARY, DISCUSSION, CONCLUSION AND RECOMMENDATIONS		56
5.1	Introduction	56
5.2	Summary of Findings.....	56
5.3	Discussion	58
5.4	Conclusion.....	59
5.5	Recommendations.....	60
5.6	Suggestions for Further Research.....	60
 References.....		61
APPENDIX I: Letter of Transmittal and Informed Consent		64
APPENDIX II: Survey Questionnaire.....		65

ABSTRACT

The pursuit of information security is characterized by practices aimed at maintaining a desired level of Confidentiality, Integrity, and Availability of information systems and assets. Rapid development of automation processes and the penetration of the computers in all fields of life have led to appearance of a range of peculiar problems. One of these problems is the necessity of providing effective protection to information. This research work was investigating the factors influencing the level of Information Security practice in state corporations in Kenya. Information Security Practices and guidelines will play a key role in identifying the factors that influence their effective implementation. With the level of information security in state corporations in Kenya in mind, the researcher explored the factors that influence the level of information security in these organizations as they implement the information security practices and guidelines. Variables such as access control mechanisms, information security management tools and technology usage, human factors in information security, security infrastructure, government regulation and past security breaches were examined so as to ascertain the level of information security derived. The findings have indicated that access control mechanisms, human factors in information security, information security management tools and technology usage and availability of security infrastructure all influences the level of information security practice in state corporations. The state corporations need to strengthen the effective implementation of the information security practices in Kenya to be able to protect their information assets as well as comply with regulatory requirements. The study has revealed that there is need to improve on areas such as screening of information security teams, development of information security policy, development and implementation of business continuity plan and disaster recovery plans, allocation of adequate budget and conformity to regulatory requirements.

CHAPTER ONE

INTRODUCTION

1.1 Background of the Study

The pursuit of information security is characterized by practices aimed at maintaining a desired level of Confidentiality, Integrity, and Availability of information systems and assets.

Rapid development of automation processes and the penetration of the computers in all fields of life have lead to appearance of a range of peculiar problems. One of these problems is the necessity of providing effective protection to information.

A lot of ways to access information, considerable quantity of qualified specialists, vast use of special technical equipment in social production make it possible for violators practically at any moment and in any place to gain access to information. As a result, the security considerations associated with information have grown more complex. With every network connection, the reach of a hostile agent becomes broader. The extent of interconnectivity of systems is such that computer viruses can be seen sweeping the globe much like the influenza biological virus. As a result, poor security practices at one company can have worldwide impact.

As if protecting data across applications, networks and mobile devices was not complex enough, social networking by employees is presenting organizations worldwide with a new and growing frontier of risk. The risks, from an information security perspective, include the loss or leaking of information; statements or information that could damage the company's reputation; activity such as downloading pirated material with legal and liability implications;

identity theft that directly and indirectly compromises the company's network and information; and data aggregation in building up a picture of an individual to mount security attacks through social engineering. (GSISS 2011)

The challenge of information security in the modern context is significant. Interconnectivity of businesses is increasingly required in order to remain competitive and function in the global economy, and yet every connection adds to the vulnerability of the system to hackers, criminals, terrorists and even the security organs and military forces of foreign governments. Risks of successful theft, compromise, and misuse or destruction of valuable information assets by insiders is also increased as connectivity increases.

A recent and global attention-getting examples of information security breach was seen in the penetration of the World Bank 18 servers in April 2010 at the highly restricted treasury unit by some Chinese hackers and gained full access to the rest of the bank's network for nearly a month and sensitive data stolen (DISC, 2010); and Honda Motor Company server attacks where thieves gained access to information belonging to 2.2 million car owners and collected e-mail addresses and vehicle identification numbers for customers (Tuan, 2011).

Within the African region, a fraudster siphoned more than US\$ 50,000 from unsuspecting travellers by buying tickets from Air Namibia and South Africa Airways using credit card fraud (Renthia, 2011). Recognition of the implications of this pervasive information security breaches has been reflected at the national level, such as the article covered in the CIO Magazine; "There is dramatic increase of hacking of websites in Kenya. The finance ministry website was brought down by hackers for 2 days and in the past year a number of websites have been compromised including statehouse.co.ke, administrationpolice.go.ke, Kenya

government portal, department of defence and Kenya airways” (CIO December 2010). Information security is a critical element of national security and national level policy makers are justifiably concerned about the state of information security in the nation.

There have been a number of surveys conducted over the last decade that have attempted to characterize the state of ISP. These surveys have been largely based on questionnaires targeted at information technology professionals working in large private sector companies. In no case has an evaluation been performed on the factors influencing the ISP in the public sector corporations. As a result, it is impossible to state any description at all on the factors influencing the ISP and understanding in a significant part of the economy of Kenya.

The research will shed new light on the factors influencing ISP in that portion of the Kenyan economy’s public sector that produces 17.2% of the Gross Domestic Product: Kenya GDP - composition by sector (2009).

This research will investigate what factors influence the level of ISP in the state corporations. Specifically, this study will identify factors influencing the level of ISP in state corporations within the ministry of industrialization. The results of this study will provide data to assist the development of public policy, educational programs, and technology in support of information security goals.

A considerable number of studies have been conducted on information security in the public sector. According to Ndung’u (2004) the information security is higher for companies that have framework for and carry out internal information security management system audits compared to those who don’t carry out such audit activities. Ryan (2001) examining the state

of ISP among public sector in the United States is fairly spotty which confirms a similar global conclusion.

In Kenya, several websites in the public sector have been compromised such as the Department of Defense, Kenya Government Portal, Administration Police, State House and more recently, The Treasury. This calls for further research to build on the existing state of ISPs.

In his research, Julie (2001) conducted an investigation on attitudes and experiences of business with regard to ISPs and indicated a positive association between the experiences and human behavior. Harry (2010) notes that for ISP to be effective, organizations should ensure that management processes identify and monitor significant factors that influence ISPs.

As the world moves more firmly into the knowledge age, the nation needs to assure the security of its national information infrastructure. Programs advocating information security, policies governing information security activities, and regulations requiring specific types of information security activities in specific industries could possibly all contribute to the assurance of the security of the national information infrastructure? In order to create such policy frameworks or regulatory structures, policy makers and leaders need to understand the current factors influencing ISP.

1.2 Statement of the Problem

With the dramatic increases of hacking of websites in Kenya and state of data and information compromised, ISPs needs to be re-examined and strengthened. Ryan (2001), in his conclusion on the research on state of ISP, indicated that further research must be performed to discover the influencing factors for effective ISP organizations. This research seeks to investigate the factors influencing the level of ISP in state corporations in Kenya.

However the research will focus on the digital information within the Ministry of Industrialization

1.3 Purpose of the study:

The purpose of this research is to establish the factors influencing ISPs in State Corporations.

1.4 Research Objectives:

The study was guided by Five objectives.

1. To establish the extent to which access controls influence the level of ISP
2. To establish the extent to which human factors influence the level of ISP
3. To establish the extent to which use of information security management tools influences the level of ISP
4. To assess how information security technology usage influences the level of ISP
5. To establish the extent to which the availability of security infrastructure influences the level of ISP

1.5 Research Questions:

The research sought to answer the following questions:

1. How does access controls influences the level of ISP?
2. To what extent does a human factor influence the level of ISP?
3. To what extent does information security management tool usage influence the level of ISP?
4. How does information security technology usage influence the level of ISP?
5. To what extent does the availability of security infrastructure influences the level of ISP?

1.6 Significance of the study:

Previous studies and surveys have revealed that public sector have put in place certain ISPs. The significance of this study lies principally in the fact that despite these practices being in place and implemented, cases of information security breaches are on the rise within the public sector.

The data provided by this study will act as a baseline on factors that influence effective ISP.

This will enable the policy makers and leaders with an understanding of how public sector contributes to or detract from the security of the national information infrastructure.

The data also provides technologists with insights into how widely used various technology solutions are in the public sector.

Management theorists will be provided with data on how management tools are used in public sector to help manage the information security challenges.

This first set of descriptive data can serve as a baseline for trend and change analysis in future studies.

1.7 Delimitations of the Study:

This study will have several delimitations. It will be delimited to the conceptualization of the factors influencing the level of ISP in the public sector. The public sector was chosen due to the high increase of information security incidences in the recent past.

The focus of this research is on factors influencing information security practise in public sector. The scope includes describing with respect to public sector:

1. What percent have information security management tools?
2. What percent have experienced information security breaches and involved?
3. What percent have information security infrastructure available?
4. What percent have experienced unauthorized access to their information systems?
5. What information security Technology usage deployed and
6. What percent of the past breaches were as a result of human factors?

The research data will be based on all ICT and Information Security personnel in the 9 state corporations in the Ministry of Industrialization, Kenya.

The time period between pre-and post-assessment was delimited to six months. This study was delimited to a questionnaire survey to CIO's and staff involved in ISP implementation.

1.8 Limitations of the Study

This study will have some limitations. One limitation is lack of accuracy of responses on the past security breaches. Respondents may not report the accurate number because they do not want to be viewed as porous security wise. Also, information security staff may not want to accurately report on sensitive questions such as access methods, information security technology usage and management tools. Since this study will not have a control group, another weakness will be the lack of control for other variables that may have influenced the level of ISP. Finally, the research describes factors influencing the level of ISPs without attempting to evaluate or describe information security requirements and ISPs implemented by the organizations. This area might provide fruitful area for research in the future.

1.9 Basic Assumptions of the Study

This study will be grounded on three assumptions namely:

1. The conceptual framework is an accurate reflection of the phenomenon to be studied.
2. The data collection instrument and data analysis will adequately capture core concepts in ISPs.
3. Findings to accrue from this study will have worth to the contemporary information security industry and the millions would be information security practitioners and clients.

1.10 Definitions of Significant Terms

Access Methods: A mechanism implemented by the organizations under study that controls the transfer or retrieval of stored data / information by an authorised person.

Information System Management Tools: Management tools adopted with respect to policies, procedures, planning efforts and audit trails to help organizations under study manage information security related problems.

Information System Technology usage: Technological tools implemented with respect to anti-virus software, data backup, firewall deployment, encryption and intrusion detection system to help organizations under study prevent information security related breaches.

Human Factors: Non- technological factors that will influence the level of ISP within the organizations under study. In this study the human factors considered are separation of duties, screening, training and awareness, user account management, top management support and competency of security team.

Level of Computerization: The extents to which the organizations under study are using computers to capture, process, store, retrieve and control data and information

Security Breach: Internal or external act that by passes or contravenes organization's security policies, practices or procedures

Information System Practice: Types of controls, objectives and procedures that organization's under study have implemented to enhance information security.

Information security: Protecting information and information systems deployed by the organizations under study from unauthorized access, use, disclosure, disruption, modification or destruction.

Interconnectivity: Concept that requires all parts of a system interact with and rely on one another within the organization and outside.

1.11 Organization of the Study

The entire research document is divided into five chapters namely, Introduction, Literature Review, Research Methodology, Data Analysis Presentation and Interpretation, Summary Discussions Conclusion and Recommendations.

**UNIVERSITY OF NAIROBI
KIKUYU LIBRARY
P. O. Box 92
KIKUYU**

CHAPTER TWO

LITERATURE REVIEW

2.1 Introduction

This chapter reviews the factors influencing the level of ISP by assessing the definitions and views of other researchers and numerous authors. Since the research is more concerned about the factors influencing the level of ISP, the literature also looks at the concept of ISPs. As predicted in the security journal - *Information Security Management*, Krause, (1993) indicated the practice of information security has become much more complicated and the need for qualified information security professionals has become critical.

The review is organised in eight broad sub sections covering all the identified variables in the research.

2.2 The Concept of Information Security

The path to ISP implementation follows the concept of CIA-- Confidentiality, Integrity, and Availability. Well, without any one, or in fact all of them, business operations, transactions, and communications can become unreliable, untrustworthy, and uncertain. CIA is a significant element in information and data security and in keeping the users of the information and data satisfied. There are different definitions and competing views of the concept of CIA as seen here below

2.2.1 Confidentiality

This means, at the core of the concept, that the data is hidden from those that are not supposed to see it.

Miller, (2006) defined confidentiality as process of limiting information access and disclosure to authorized users -- "the right people" -- and preventing access by or disclosure to unauthorized ones -- "the wrong people."

Underpinning the goal of confidentiality are authentication methods like user-IDs and passwords that uniquely identify an information system's users, and supporting control methods that limit each identified user's access to the information system's resources

We can accomplish Confidentiality in a number of ways. These methods are complementary. First, require strong authentication for any access to information. Second, use strict access controls. In communications only the sender and intended recipient should be able to access the data.

2.2.2 Integrity

Integrity as a concept means that there is resistance to alteration or substitution of data, and/or that such changes are detected and provable. The information should not be changed except by an authorized agent. Whether the data might be changed by accident or malice, preventing that change is the foremost concern, and detecting if it has changed is second. Integrity can be maintained at many levels, from the hardware all the way to the application logic.

ISO 27001 (2005) defines integrity as a systematic process that safeguards the accuracy and completeness of information and processing methods. This ensures continuity and restoration of your business in case of disaster

2.2.3 Availability

For our data/information to be of use to us, it has to be accessible when and where we need it. Therefore part of the puzzle is how to keep our data available. Attacks or accidents can bring down systems. Data can be overwritten, deleted, or destroyed. Denial of Service attacks can make otherwise fast-access systems run like cold molasses.

High Availability solutions, including load balancing, fail-over, and quick backup and restoration are all involved.

Almost all modern organizations are highly dependent on functioning information systems. Many literally could not operate without them.

Availability, like other aspects of security, may be affected by purely technical issues (e.g., a malfunctioning part of a computer or communications device), natural phenomena (e.g., wind or water), or human causes (accidental or deliberate).

Lopez, (2009) in International Journal of Information Security defined availability as the property of being accessible and usable upon demand by an authorised entity.

2.3 Information Security Practice

Businesses operate in an environment with increasingly powerful ways of manipulating and storing information. This is matched by growing threats to that information. Businesses need

to manage their information so that they get the best value from it, and minimise the risks of losing it.

Information security is necessary to ensure that your business can continue to operate effectively and profitably. ISO/IEC 27001 standard defines the various ISPs that organizations should implement. The practices guide organizations on the types of controls, objectives and procedures that comprise an effective IT security program. The practices show what should be done to enhance or measure an existing computer security program or to aid in the development of a new program. The practices provide a common ground for determining the security of an organization and build confidence when conducting multi-organizational business. Swanson and Guttman, (2006) emphasises that organizations should use the practices as a starting point in order to develop additional practices based on their own organizational and system requirements. The common practices should be augmented with additional practices based on each organization's unique needs.

2.4 Access Controls Mechanisms

Access control is only one subset of factors influencing level of ISP. In addition to implementing ISPs, organizations must define control measures and implement them to be able to control access to their information.

According to Dubin (2006), there are four key areas that define access controls broken down as follows:

- a. Identity administration sets up user roles and groups that allow access only to authorized systems.
- b. Identity infrastructure is the data store that holds user accounts and identity information, such as Active Directory.

- c. Access management sets up user accounts with user IDs and passwords, or whatever system is used for access, like smart cards or biometrics.
- d. Finally, auditing is about reporting on accounts, such as who has access and to what systems and at what time did they access what.

ISO/IEC 27001 (2005), under controls and control objectives, establishes an access objective to prevent unauthorized physical access, damage and interference to the organization's premises and information. This is achieved by defining controls for five key areas namely physical security, securing facilities, protection against external and environmental threats, working in secure areas and public access.

Access control to ISO/IEC 27001 (2005) standard involves defining the above controls and implementing them.

According to Auerbach publications (2011), deployment of access control mechanisms and verification of the identity of a user (authentication) before full access to resource is granted are key to successful implementation of access control.

2.5 Information System Management Tools Usage

Every organization recognises the importance of securing their information systems that are now at the heart of many business processes. This recognition goes beyond simple deployment of security technologies.

According to Lock (2010), drivers such as compliance with regulatory pressures, minimising financial risks, securing corporate data and protecting a company's brand are all important

aspects of what we might term 'Information System Security' today. No wonder, then, that its significance in continuing day to day operations is now recognised as a fact of life.

This recognition places greater stress on the overall management strategies that organisations need to secure Information system operations. Such strategies generally depend upon using systems and security management tools effectively; the alternative is to implement labour intensive processes using scarce human resources.

Ndungũ (2004) reported that organisations are looking to continuously deploy new and updated services and to make use of an ever-growing range of tools and devices. Specialist tools do exist to deal with security itself, but we are seeing pressure from various quarters to consider security as one element of the broader Information system management discipline.

Against this background, then, how should Information system security be tooled up? Perhaps the most obvious starting point is to revisit some of the solutions at the heart of good systems management, with respect to their specific security role. Amongst these are, for example, identity management, asset management and data classification technologies. Where do these capabilities fit from a security perspective, as organisations look to deploy new solutions and work in rapid response to volatile business conditions?

According to Lock (2010) identity management has the most obvious direct connection to securing Information Systems operations and services. Few organisations have implemented identity management policies and solutions that can span the entire Information systems infrastructure, so its role in security management will be inevitably limited as a result. Even fewer have policies or tools in place capable of working with identities of individuals outside of the organisation who may require access to corporate information.

Meanwhile, the potential benefits of using well maintained asset management tools to help secure the organisation have not been widely recognised in the security sphere. Yet a little thought illustrates how the asset / inventory / configuration information held in such repositories can be exploited to support the management of security as a whole.

Felicia (2011) in Information System Security journal remarked that simply checking that operating systems and applications are running the latest patches has obvious security benefits, especially when you take into account that identifying un-patched machines without such tools is both time consuming and prone to manual errors. Knowing who is using which machine and whether the device is loaded with the software appropriate for the job could also help highlight areas of potential exposure. This can be aided by ensuring that all software utilised in the business is properly licensed: not only knowing what you have, but also paying for the requisite levels of software assurance, patching and support all contribute to minimising risk.

The final example of using systems management tools to help ensure security management policies are enacted in the real world, concerns data classification. According to Nicastro (2011), increasing amounts of sensitive corporate data are being held outside of central storage platforms, for example on laptops and mobile devices. Unless the organisation has some means, manual or automated, of establishing the sensitivity of data or information held on such machines it is a difficult task to ensure that sensitive data is adequately secured and protected. However, with new disclosure legislation looking likely in various countries, together with increased penalties for data loss and data breaches, organisations are under increasing pressure to do so.

So, there are systems management tools available which can help raise the level of security in Information Systems services delivery, but this approach can only take things so far as such tools were not designed specifically for the job. If the tools offer only the means and not the end, this raises the challenge of how to ensure that security management needs are comprehensively covered, particularly if the potential use case scenarios are not widely understood outside the domain of security specialists?

Ryan (2001) concludes that on the way forward, one might naively assume, would be to get the experts together – for example bringing together specialist staff from a compliance monitoring department to work with systems management staff within the business, or employing external consultants who have done it before.

CIO East Africa (January 2011) reports that the most commonly used information system management tool is data recovery procedures, followed by information security policy. While data recovery procedures was the most commonly selected management tool, both data and media destruction procedures were rarely indicated. It further reports that less than 30% of organizations have a Disaster Recovery Plans.

2.6 Information System Technology Usage

Recently usage of information system technology has been studied as a phenomenon of interest in its own right. (Davis 1993; Hartwick and Barki 1994). As a key variable in information system security practice research literature, understanding usage is of the increasing theoretical interest. It is also of increasing practical importance as the usage of information systems security practice becomes more pervasive. From a more pragmatic point of view, understanding the determinants of information system technology usage should help to ensure effective deployment of information system security resources in an organization.

Such usage is a necessary condition for ensuring security to information systems (Davis 1989).

According to Todd (1995), in recent years, a variety of theoretical perspectives have been advanced to provide an understanding of the determinants of usage. Focus on the identification of the determinants such as attitudes, social influences and facilitating conditions (Mathieson 1991)

Information Systems Technology usage has emerged as powerful and parsimonious way to represent the antecedents of information systems technology usage through beliefs about two factors: the perceived ease of use and the perceived security of an information system (Davies et al. 1992). The practical utility stems from the fact that ease of use and security are factors over which systems designers has some degree of control. To the extent that they are key determinants of usage, they provide direction to designers as to where efforts should be focussed.

According to Moore (1993) the four most frequently indicated technologies used were anti-virus software, data back-up systems, system access controls, and encryption. Each of these technologies are used by more than seventy percent of the organizations.

2.7 Human Factors in Information Security Practice

According to Felicia (2011) People, process, and technology are all common aspects to any information system security process implemented within an organization. The three aspects can be thought of as gears, all required to work together to accomplish the task successfully. They must also be aligned properly within the organization when it comes to the patch management process. Of course, this can be applied to all the processes within an

organization. The *people* aspect is self-explanatory; it is the individuals responsible for confirming that a task has been completed. They may be management providing the support required to ensure that the process is established and adhered to properly by all individuals required. The operational personnel provide input and guidance into the process. They may be the ones driving the process or seeing the need to create one. The operational personnel may provide the rest of the group with guidance on how the process should be designed or some of the requirements that the process must meet. The technical personnel are the ones who may complete an actual task. They may be the ones following the procedures established within the process, such as deploying the patch to the vulnerable systems. People come into play at various intervals within a process through the ownership, establishment, and day-to-day operations of the process itself

Thinking personally, have you ever entered a value in the wrong field on a form, or put the decimal point in the wrong place? Deleted the wrong file by mistake? Pulled out the wrong plug? Simple mistakes like this are so commonplace, we mostly just accept them as inevitable and do our best to spot and correct the problems before it is too late. In the context of information security, simple configuration mistakes can leave network ports open, firewalls vulnerable and systems completely unprotected. We contend that human error is far more likely to cause serious security breaches than technical vulnerabilities.

Hinson (2003) argues that technical flaws are themselves the product of human errors: do you remember the case of the radiotherapy machine that delivered ten-times the stated dose? This was traced to an obscure bug in the program that somehow escaped rigorous testing. Human beings were to blame for the machine's faults.

There is a field of science called "human factors engineering" that seeks to address the problem.

In some cases (*e.g.* power station control systems), 'pressing the wrong key' can have such disastrous effects on safety that special controls are required to reduce the risk. There are system interlocks, dual controls and automatic programmed responses. Whole banks of monitors keep a constant check on the systems and their operators, and respond dynamically to alarm conditions.

According to Garry (2003) safety-critical systems are designed, developed, tested, operated and maintained with human safety very much in mind ... and yet mistakes still occur. Power station operators sometimes press the wrong buttons, shut down the wrong systems and cause safety incidents.

Sports car drivers sometimes turn off their sophisticated traction control systems to 'have more fun', and occasionally exceed the capabilities of the anti-skid braking systems.

On another tack, Kevin (2003) demonstrated just how easy it is to persuade naive helpdesk staff to give out sensitive information over the phone to complete strangers. Users choose weak passwords and resent having to change them regularly. They share IDs. They forget their smartcards. Whilst system controls can sometimes help (*e.g.* enforcing long alphanumeric passwords), users still have to play their part (*e.g.* not using simple keyboard patterns).

In a nutshell, information security is both a human and a technological problem.

2.8 Security Infrastructure

Although some levels of computing services are provided in a centralized manner, administration of desktop computing and other specialized services are usually provided and supported by local computing departments. The potential increase in the number of security-related incidents in organizations as well as state-wide data security audits has resulted in the

need for centralization and coordination of security efforts and implementation of a security structure organization-wide to facilitate the dissemination of information and identification of appropriate personnel in each computing department to address security threats quickly and efficiently (USF Journal 2008).

According to 360 Information Security Journal (2010), Information Systems security like physical security, is most cost effective when designed-in from the outset. However not every company has the foresight to do this and many organizations still do not have security as a primary concern when deploying their information systems infrastructure. The networking boom of the late 90's resulted in the rapid deployment of thousands of servers, switches, and applications as companies connected to the Internet, automated supply chains and issued laptops to mobile workers. Little thought was given to the likely ongoing cost of managing security for this huge new infrastructure.

Today Information Systems managers face increasing malicious activity, a stricter regulatory environment, and a new awareness of personal privacy issues by their customers. This is reflected in the explosion in reported incidents to the Computer Emergency Response Team (CERT).

By re-visiting the design of your existing information systems security and following best practices in new deployments you can gain maximum benefit while making ongoing management less draining. Having a clear architecture, and making the most appropriate use of products and services you can reduce your exposure to risk while being able to 'do more with less' (360 Info Sec 2010).

According to a publication by Georgia Technology Authority (2008), each organization has the responsibility to exercise due diligence and due care in support of the organization's

commitment to protecting its information assets, as well as for compliance with state regulatory requirements.

Any organization that creates, uses, or maintains information assets, shall also establish, document, implement and maintain an internal information security infrastructure consisting of the following program elements:

- a. A Security management organization
- b. A risk management framework consistent with that recommended by the National Institute of Standards and Technology (NIST)
- c. A Disaster Recovery Plan
- d. An Incident Management and Response capability
- e. Security Education and Awareness component
- f. Internal policies and procedures necessary to meet organization's specific business security needs or augment security requirements imposed on such organization by state regulations.
- g. Assessment, Compliance and Enforcement mechanisms

2.10 Conceptual Framework

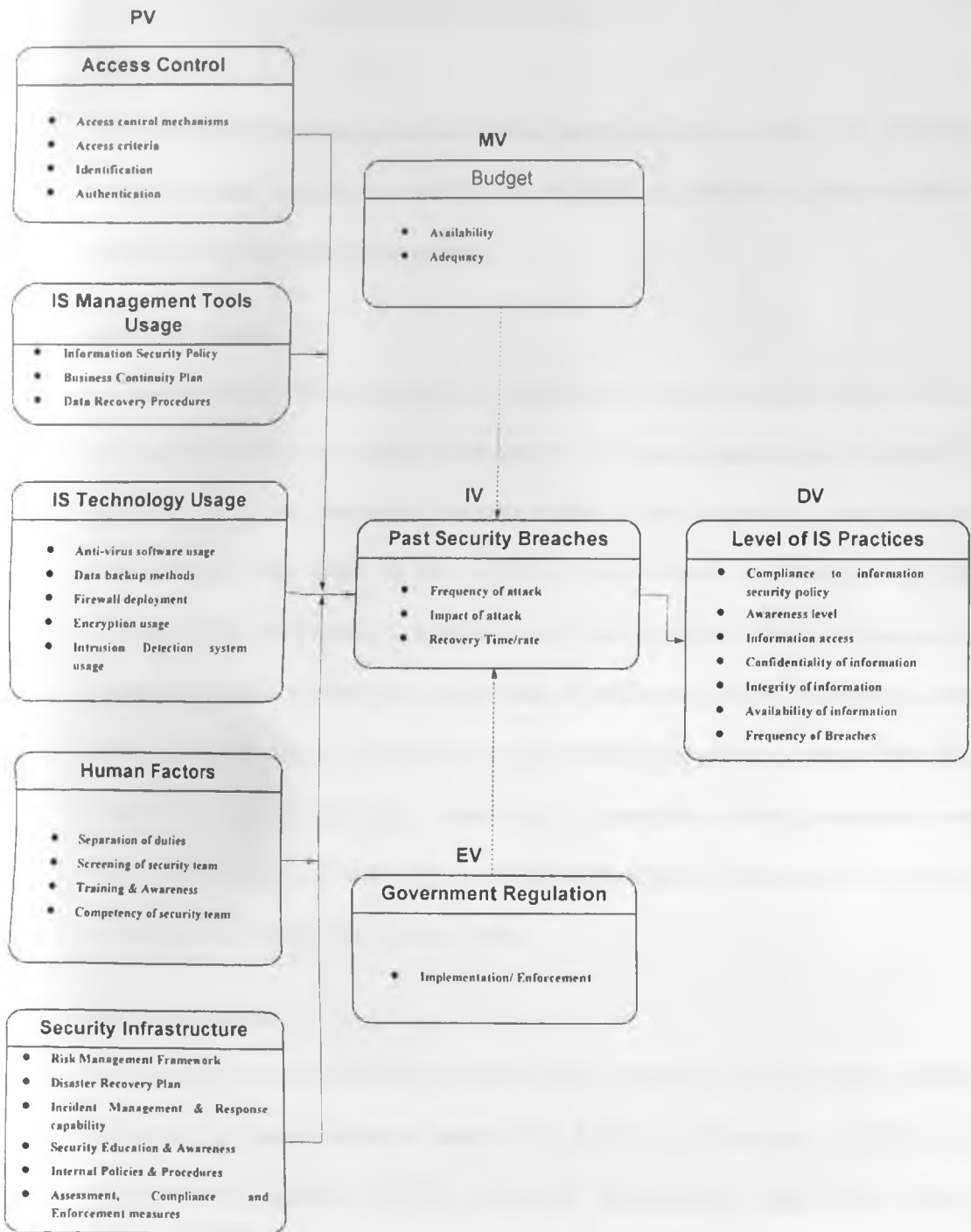


Figure 1 Conceptual Framework

Source: Author 2012

CHAPTER THREE

RESEARCH METHODOLOGY

3.1 Introduction

This section outlines the researchers design, target population, sample size, sampling design, research instruments, validity and reliability of instruments, data collection procedure and data analysis procedure.

3.2 Research Design

A research design is the arrangement of conditions for collection and analysis of data in a manner that aims to combine relevance to the research purpose with economy in procedure. It is the conceptual structure within which research is conducted. It constitutes the blue print for the collection, measurement and analysis of data (Kothari, 2003). In this study descriptive survey was employed. The major purpose of descriptive survey is description of the state of affairs as it exists at present in this case the researcher has no control over the variable, one can only report what has happened or what is happening. Generally, in a descriptive survey, researchers are not so much concerned with why the observed distribution exist as with what the distribution is (Fraenkel and Wallen, 2008).

3.3 Target Population

The target population for this study included firstly, nine (9) state corporations within the Ministry of Industrialization namely, Kenya Bureau of Standards (KEBS), East Africa Portland Cement (EAPCC), Industrial Development Bank (IDB), Kenya Industrial Research Development Institute (KIRDI), Kenya Industrial Property Institute (KIPI), Industrial & Commercial Development Corporation (ICDC), Numerical Machining Complex (NMC), Kenya National Accreditation Service

(KENAS) and Anti Counterfeit Agency (ACA). Secondly, it included all Information Security Staff within each of the nine (9) State Corporations of the Ministry of Industrialization. According to staffing levels of Information & Communication Technology staff and staff involved in ISP collected from all the nine (9) state corporations, the target population was all ISP staff estimated at about 105 members of staff.

3.4 Sampling Procedure and Sample Size

Census method was used to collect feedback from the respondents. The researcher used census method because of the small target population involved and wanted to give everyone an opportunity to give feedback and to help increase the statistical confidence. 100% sampling (all) was taken into account for corporate target population involving Information and Communication Technology staff and staff members involved in ISP.

According to Fraenkel and Wallen, (2008) an occasion, based on previous knowledge of a population and the specific purpose of the research, investigators use personal judgement to select a sample. In this research sampling was done as shown in the table below:

Table 3.1: Sampling Frame

Category	Population (ICT & Information Security staff)	Sample	%
KEBS	22	22	20.9
ICDC	19	19	18.2
ACA	10	10	9.5

EAPCC	10	10	9.5
IDB	9	9	8.6
KENAS	10	10	9.5
KIPI	8	8	7.6
KIRDI	9	9	8.6
NMC	8	8	7.6
Total	105	105	100

Source: Author 2012

3.5 Methods of Data Collection

The administration of research data collection instruments was done by the researcher during the study. The researcher sought a research permit from the office of the Permanent Secretary, Ministry of Industrialization.

After obtaining the permit, the researcher contacted the CIOs or responsible persons. The researcher then made a list of the respondents to be interviewed. Before proceeding to the field, telephone calls were made (where possible) to book appointments. Once contact was established, the questionnaires were self administered.

During the data-gathering exercise, respondents were assured of strict confidentiality in dealing with their responses. This demanded the researcher to create a rapport with the respondents, so as to gain their acceptance and trust. To ensure full co-operation, from the respondents the researcher explained the significance of the study and their participation.

Where situations did not allow for self administering of the questionnaire, the researcher left them with the respondents then made arrangement as to when they were to be collected for analysis.

Data collection tools or instruments used were questionnaires and interviews. The survey was carried out from the month of May for 2 months.

3.6 Validity And Reliability

The researcher checked the Validity and Reliability of the research instrument as detailed below:

3.6.1 Instrument Validity

Validity is the accuracy and meaningfulness of inferences, which are based on the research results. It is the degree to which results obtained from the analysis of the data actually represent the phenomenon under study (Mugenda and Mugenda, 1999). To enhance the validity of the instruments, the questionnaires were reviewed by a panel of experts made up of the University supervisors and lecturers, on validity and relevance of the questions to the topic under study. Any alterations required were incorporated in formulating the final copy of the questionnaire.

3.6.2 Reliability of the Instrument

Reliability refers to the consistency of the scores obtained; how consistent they are for each individual from one administration of an instrument to another and from one set of items to another (Fraenkel and Wallen, 2008). Roscoe (1969) states that the half-split method during the pre-test can be used to establish the internal consistency (coefficient of test). Nachmias and Nachmias (1976), Lokesh (1984) and Gall, Borg and Gall (1996) concur with this.

st reliability of the instrument the researcher used the split-half technique. By this method the researcher aimed at determining the co-efficient of internal consistency or reliability co-efficient whose value varied between 0.00 (indicating no reliability) and +1.00 (indicating perfect reliability). Piloting of the questionnaire was with 25 respondents at KEBS to help ascertain whether research objectives be met and the outcome of the piloting were incorporated in the refining process questionnaire.

3.7 Operational Definition Of Variables

Objective	Variables	Indicators	Measurement	Measuring Scale	Research Design	Type of Analysis	Analysis Tools
To establish whether access methods influence the level of ISP	Independent: Access Control	<ul style="list-style-type: none"> • Access control mechanisms • Access criteria • Identification • Authentication 	Degree of control	Interval	Quantitative	Descriptive	Median
	Dependent: Level of IS practice	<ul style="list-style-type: none"> • Compliance to IS policy • Awareness level • CIA of information • Frequency of breaches 	Level	Ordinal	Quantitative	Descriptive	Median

<p>To establish the extent to which human factors influence the level of ISP</p>	<p>Human Factors</p>	<ul style="list-style-type: none"> • Separation of duties • Screening of Security Teams • Training & Awareness • Competency of Security Team 	<p>Level</p>
<p>To establish the extent to which use of information security management tools influences the level of ISP</p>	<p>Information Security Management Tools Usage</p>	<ul style="list-style-type: none"> • Security Policy • Business Continuity Plan • Disaster Recovery Procedure 	<p>level</p>

Ordinal	Quantitative	Descriptive	Median
Ordinal	Quantitative	Descriptive	Median

<p>To assess how information security technology usage influences the level of ISP</p>	<p>Information Security Technology Usage</p>	<ul style="list-style-type: none"> • Anti – virus • Data Backup • Firewall • Deployment • Encryption • Intrusion Detection System 	<p>Level</p>	<p>Ordinal</p>	<p>Quantitative</p>	<p>Descriptive</p>	<p>Median</p>
<p>To establish the extent to which the availability of security infrastructure influences the level of ISP</p>	<p>Security Infrastructure</p>	<ul style="list-style-type: none"> • Risk Management • Disaster Recovery Plan • Incident Management & Response • Security 	<p>level</p>	<p>Ordinal</p>	<p>Quantitative</p>	<p>Descriptive</p>	<p>Median</p>

		Education & Awareness <ul style="list-style-type: none"> • Internal Policies & Procedures • Assessment, Compliance & Enforcement 	
--	--	--	--

Table 3.2 Operational Definitions of Variables

3.8 Methods Of Data Analysis

After the data was collected, the first step for the researcher was to scrutinize the instrument for completeness, accuracy and uniformity. The next step was coding the data. The purpose of coding was to classify the answer to a question into meaningful categories so as to bring out their essential pattern. The researcher used statistical package for social sciences (SPSS) to generate frequency distributions using descriptive statistics in order to examine the pattern of the responses. The findings was presented in the form of tables, frequencies and percentages because they could easily bring out the relative differences of values

3.9 Summary

As indicated above, the steps were undertaken to ascertain the factors influencing the level of ISP in public sector. Data was thoroughly scrutinized with very high degree of accuracy. With these premises obtained, we can be able to conclude on status of ISP in Public sector.

CHAPTER FOUR

DATA ANALYSIS, PRESENTATION AND INTERPRETATION

4.1 Introduction

The pursuit of information security is characterized by practices aimed at maintaining a desired level of Confidentiality, Integrity, and Availability of information systems and assets. The purpose of this research was to establish the factors influencing ISPs in State Corporations. This chapter presents the findings of the study.

4.1.1 Questionnaire Return Rate

Out of 101 questionnaires distributed to the Information & Communication Technology staff and staff involved in ISP; four (4) were not administered/collected back. The shortfall of this 4 number was because the respondents were away from office during self-administering process. This total number of 101 (96.1%) is above the threshold for a normal distribution for measures of central tendency such as mean, median and mode, and, as such can be used to inform on the population it was drawn from.

4.2 Background Characteristic Of Respondents

The background characteristics of the respondents are presented in Tables 4.1- 4.4. These include type of the respondent, gender, age and marital status.

4.2.1 Organization

As shown in Table 4.1, majority (21.8 %) of the respondents are drawn from the Kenya Bureau of Standards (KEBS) followed by Industrial and Commercial Development Corporation (ICDC) at 18.8 %. Anti-Counterfeit Agency (ACA), East African Portland Cement Company (EAPCC), Industrial Development Bank (IDB) and Kenya National Accreditation Service (KNAS) all have the same proportion of respondents (8.9 %). Equally, Kenya Industrial Property Institute (KIPI) and Kenya Industrial Research Development Institute (KIRDI) have the same proportion of respondents (7.9 %).

Table 4.1: Organization of the respondent

Respondents	Frequency	%
Anti-Counterfeit Agency	9	8.9
East African Portland Cement Company	9	8.9
Industrial and Commercial Development Corporation	19	18.8
Industrial Development Bank	9	8.9
Kenya Bureau of Standards	22	21.8
Kenya Industrial Property Institute	8	7.9
Kenya Industrial Research Development Institute	8	7.9
Kenya National Accreditation Service	9	8.9
Numerical Machining Complex	8	7.9
Total	101	100.0

Source: Author 2012

4.2.2 Position of the respondent in the organization

Table 4.2 presents the positions/designations of the respondents. Response to this question was poor and only 18 respondents stated their positions/designations. Majority of the respondents were either help desk assistant or system administrators (3 %).

Table 4.2: Position of the respondent

	Frequency	%
Chief ICT Manager	1	0.9
Developer	2	2.0
Help Desk assistant	3	3
ICT Manager	1	0.9
Manager Systems	2	2.0
Network Administrator	1	0.9
Programmer	1	0.9
Server Administrator	1	0.9
Support Assistant	1	0.9
System Administrator	3	3
Technician	1	0.9
Webmaster	1	0.9
No response	83	82.2
Total	101	100.0

Source: Author 2012

4.2.3 Age bracket of the respondent

The age bracket of the respondents is presented in Table 4.3 below. More than two thirds (66.3 %) are between 31-40 years old, followed by 41-50 years and 18-30 years (19.8 % and 10.9 % respectively). Only 3 % are above 50 years.

Table 4.3: Age bracket of the respondent

	Frequency	%
18-30	11	10.9
31-40	67	66.3
41-50	20	19.8
Above 50	3	3.0
Total	101	100.0

Source: Author 2012

4.2.4 Information security role of the respondent

As shown in Table 4.4. Only 8 responded to the question on information security role of the respondent. However, 5.9 % are implementers of information security while system administrators and technical committee are each represented by 0.9 %.

Table 4.4: Information security role of the respondent

	Frequency	%
Implementer	6	5.9
System Administration	1	0.9
Technical committee	1	0.9
No Response	93	92
Total	101	100.0

Source: Author 2012

4.3 Access Control

One objective of the study was to establish whether access controls influence the level of ISP. The access controls considered in the study included the presence of access control and access control mechanisms. The findings are discussed below.

4.3.1 Presence of access control

In establishing the presence of access controls, the study sought to know availability of access control mechanisms, presence of access criteria and user of information identification among the state corporations. The results in Table 4.5 shows that most state corporations (75.2 %) have access control mechanisms. Similarly majority of state corporations also have well defined access criteria and can identify user of information (66.7 % and 67.7 % respectively).

Table 4.5: Presence of access control

	Yes		No	
	Frequency	%	Frequency	%
Availability of access control mechanisms	76	75.2	25	24.8
Access criteria defined	66	66.7	33	33.3
User of information identified	67	67.7	32	32.3

Source: Author 2012

4.3.2 Access control mechanisms

Table 4.6 describes the various access control mechanisms employed by the state corporations to determine the level of ISP. The most common types of access control mechanism are passwords and restricted access (57.0 % and 26.0 % respectively). On the other hand, data encryption accounts for only 1.0 %.

In terms of access criteria used, most state corporations (40.0 %) provide access based on the roles of the employees. Passwords and access levels account for 24.6 % and 21.5 % of access criteria respectively. The least used access criteria are username and authentication (both at 3.1 % respectively).

In order to authenticate user of information, majority of state corporations (65.9 %) use passwords while 30.5 % authenticate through username of the person accessing the information. Only 1.2 % of the state corporations authenticate user of information through biometrics as shown in Table 4.6 below.

Table 4.6: Access control mechanisms

Type of access control mechanisms (n=100)	Frequency	%
Passwords	57	57.0
Physical access control	5	5.0
Computer based	1	1.0
Restricted access	26	26.0
Biometrics	7	7.0
Rights and permissions based on roles	3	3.0
Data encryption	1	1.0

Access criteria used (n=65)		
Based on role	26	40.0
Passwords	16	24.6
Username	2	3.1
Rights of admission	5	7.7
Access levels	14	21.5
Authentication	2	3.1

Methods of authenticating user of information (n=82)		
Passwords	54	65.9
Username	25	30.5
Pin	2	2.4
Biometrics	1	1.2

Source: Author 2012

4.4 Human Factors

Human factors and their influence on the level of ISP in the state corporations were studied. The factors considered are human factor determinants and measures to ensure competence of security teams' members.

4.4.1 Human factor determinants

Human factor determinants for ISP by the state corporations are conducting security awareness trainings (34.7 %), screening of information security teams before employment (15.8 %) and authorities and responsibilities defined (62.4 %) as shown in Table 4.7 below.

Table 4.7: Human factor determinants

	Yes		No	
	Frequency	%	Frequency	%
Conducting security awareness training	35	34.7	66	65.3
Screening of information security teams before employment	16	15.8	85	84.2
Authorities and responsibilities defined	63	62.4	38	37.6

Source: Author 2012

4.4.2 Competence of security team members

Competence of security teams' members in the state corporations is mostly ensured through training (43.6 %) followed by awareness creation (15.8 %) and recruiting staff with right qualifications (4 %). Frequent drilling and emerging trends each account for only 2.0 % of mechanisms used to ensure competence of security teams' members (see Table 4.8 below).

Table 4.8: Mechanisms to ensure competence of security team members

	Frequency	%
Awareness creation	16	15.8
Training	44	43.6
Right qualifications	4	4
Frequent drilling	2	2.0
Emerging trends	2	2.0
No Response	33	32.7
Total	101	100.0

Source: Author 2012

4.5 Information Systems Management Tools Usage

The study also sought to establish the extent to which use of information security management tools influences the level of ISP. Issues discussed here are information security management tools.

4.5.1 Information security management tools

Table 4.9 below shows the different information security management tools employed by the state corporations. 36.0 % of them reported having information security policy, 20.8 % had developed and implemented business continuity plan, and 29.7 % had developed and implemented disaster recovery plan while only 6.9 % reported that they have tested both continuity plan and disaster recovery plan.

Table 4.9: Information security management tools

	Yes		No	
	Frequency	%	Frequency	%
Availability of information security policy	36	36.0	64	64.0
Development and implementation of Business Continuity Plan (BCP)	21	20.8	80	79.2
Development and implementation of Disaster Recovery Plan (DRP)	30	29.7	71	70.3
Testing of both BCP/DRP	7	6.9	94	93.1

Source: Author 2012

4.6 Information Security Technology Usage

Assessment of how information security technology usage influences the level of ISP was also an objective of this study. Issues here are information security technology measures, frequency of usage and managing information security. The findings are discussed below.

4.6.1 Information security technology measures

As shown in Table 4.10, majority (89.1 %) of state corporations have installed anti-virus to protect their information from virus infections. Equally, 83.2 % have backed up their critical data.

Table 4.10: Information security technology measures

	Yes		No	
	Frequency	%	Frequency	%
Anti-virus software installed	90	89.1	11	10.9
Critical data/information backed up	84	83.2	17	16.8

Source: Author 2012

4.6.2 Frequency of usage

Frequency of usage of information security technology is presented in Table 4.11. Close to half of the state corporations (47.5 %) reported updating anti-virus daily. 19.8 % update anti-virus automatically while 9.9 % update anti-virus weekly.

In terms of data backup, 46.9 % of state corporations reported backing up their data daily while 16.3 % back up their data weekly. Additional 8.2 % automatically back up their data while 6.1 % back up data on a need basis (see Table 4.11).

Table 4.11: Frequency of usage

Frequency of anti-virus update (n=101)	Frequency	%
Automatic	20	19.8
Frequently	4	3.9
Daily	48	47.5
Weekly	10	9.9
Monthly	2	2.0
Quarterly	2	2.0
Need basis	2	2.0
Others	13	12.9

Frequency of backup (n=98)

Real-time	8	8.2
Hourly	2	2.0
Daily	46	46.9
Weekly	16	16.3
Monthly	2	2.1
Quarterly	1	1.0
Need basis	6	6.1
Others	17	17.4

Source: Author 2012

4.6.3 Managing information security

In managing information security, state corporations stated their medium of backup, how they managing intrusion to organization data/information and how they prevent organization network from public network. The most common medium for backup is disk (48.3 %) followed by tape 15.7 %. Servers and UTM each accounted for 12.4 % (see Table 4.12).

Table 4.12: Managing information security

Medium of backup (n=89)	Frequency	%
Storage	5	5.6
SAN	2	2.3
Servers	11	12.4
Disk	43	48.3
Tape	14	15.7
Internet	2	2.2
Back up memory	1	1.1
UTM	11	12.4
Total	89	100.0

Source: Author 2012

4.6.4 Managing intrusion to organization data/information

The most common way of managing intrusion to organization data/information is restricted access (33.7 %) followed by firewall (10.8 %) as shown in Table 4.13 below. Intrusion detection systems and security tools each accounted for 9.9 %.

Table 4.13: Managing intrusion to organization data/information

	Frequency	%
Firewall	11	10.8
Intrusion detection system	10	9.9
IPS	6	5.9
Passwords	4	4
Permission	4	4
Policies	2	2.0
Prevention	3	3.0
Private network	2	2.0
Restricted access/access control	27	33.7
Security tools	10	9.9
Storage	1	0.9
No Response	21	20.8
Total	101	100.0

Source: Author 2012

4.6.5 Preventing organization network from public network

As shown in Table 4.14, majority of state corporations prevent their network from public network through firewall (59.4 %). An addition 7.9 % use ISP to prevent their network from public network. Other preventive measures account for less than 5 % each.

Table 4.14: Preventing organization network from public network

	Frequency	%
Control point of entry/exit	1	0.9
Firewall	60	59.4
ICT Staff	3	3.0
Not protected	4	4.0
Passwords	1	0.9
Private IP	2	2.0
Proxy server	2	2.0
Seclusion	2	2.0
Security tools	4	4.0
Separating the networks	3	3.0
Through intranet	1	0.9
Unified threat management	1	0.9
Use of ISP	8	7.9
No Response	9	8.9
Total	101	100.0

Source: Author 2012

4.7 Security infrastructure

The last objective is to establish the extent to which the availability of security infrastructure influences the level of ISP. Issues discussed include data risk management, incident response

and management and frequency of information security awareness, presence of internal policies and procedures and information security enforcement and assessment.

4.7.1 Data Risk Management

Most state corporations manage data risk through backups (38.6 %). Control access, policies and restricted access and distribution is employed by 12.9 %, 11.9 % and 11.9 % respectively. Other data risk management mechanisms account for less than 5 % each (see Table 4.15).

Table 4.15: Data Risk Management

	Frequency	%
Back up	39	38.6
Based on management system	2	2.0
Control access	13	12.9
ICT department	2	2.0
Not defined	4	4.0
Policies	12	11.9
Protected against unauthorized access	3	3.0
Restricted access and distribution	12	11.9
Rights and permissions	3	3.0
Security controls	2	2.0
User responsibility	3	3.0
No Response	6	5.9
Total	101	100.0

Source: Author 2012

4.7.2 Incident Response and Management

The most common incident response and management mechanism used is reporting to help desk (19.8 %) followed by procedures (14.9 %) and response/management based on criticality of the incident (10.9 %) as presented in Table 4.16 below 5.9 % of the state corporations have not defined their incident response and management mechanisms. Other mechanisms apart from response/management based on classification and data recovery account for less than 10 % each.

Table 4.16: Incident Response and Management

	Frequency	%
Based on law	2	2.0
Based on classification	6	5.9
Based on criticality	11	10.9
Based on priorities	3	3.0
Reporting to help desk	20	19.8
Classified according to impact	2	2.0
Data recovery	4	4.0
Not defined	6	5.9
Procedures	15	14.9
Through different classes	3	3.0
Through indent management procedure	1	0.9
Through laid down procedures	2	2.0
Using backup software	2	2.0
No Response	24	23.8

Total	101	100.0
--------------	------------	--------------

Source: Author 2012

4.7.3 Frequency of information security awareness

More than half of state corporations (36.7 %) undertake information security awareness based on necessity (Table 4.17). An additional 13.9 % undertake information security awareness once in a while/rarely and 2.0 % never undertake information security awareness.

Table 4.17: Frequency of information security awareness

	Frequency	%
Very often	4	4.0
Quarterly	1	0.9
Bi annually	3	3.0
Thrice a year	1	0.9
Annually	2	2.0
Once in a while/rarely	14	13.9
When necessary	34	36.7
Never	2	2.0
No Response	40	39.6
Total	101	100.0

Source: Author 2012

4.7.4 Presence of internal policies and procedures

Internal policies and procedures to ensure information security are present in close to 90 % of the state corporations as shown in Table 4.18 below. The remaining corporations do not have the policies.

Table 4.18: Presence of internal policies and procedures

	Yes		No	
	Frequency	%	Frequency	%
Presence of internal policies and procedures	90	89.1	11	10.9

4.7.5 Information security enforcement and assessment

The mechanisms employed by corporations to enforce and assess information security are presented in Table 4.19 below. The most common is development of policies and procedures (51.5 %) followed by development of regulations/laws to govern information security (17.8 %). However, 4.0 % of the corporations do not have information security enforcement and assessment.

Table 4.19: Information security enforcement and assessment

	Frequency	%
Regulations/laws	18	17.8
Monitoring	4	4.0
Assigned responsibilities	2	2.0
Policies/procedures	52	51.5
Reviews	2	2.0
Access control mechanism/logs/passwords	2	2.0

Using firewalls	1	0.9
Respective managers	6	5.9
Management meetings	2	2.0
None	4	4.0
No Response	8	7.9
Total	101	100.0

Source: Author 2012

4.7.6 Level of information security practice

Table 4.20 presents the assessment of the level of ISP in the state corporations. 12.9 % reported that the information security deployed is effective while 53.5 % have experienced information security breach. The above-mentioned issues may be related to the inadequate budget allocated to the implementation of information security as shown below – only 13.8 % of the corporations have adequate budget.

Table 4.20: Level of information security practice

	Yes		No	
	Frequency	%	Frequency	%
Effectiveness of information security deployed	13	12.9	88	87.1
Experienced information security breach	54	53.5	47	46.5
Adequate budget to implement information security	13	13.8	81	86.2

Source: Author 2012

4.7.7 Conformity to regulatory requirements

Conformity to regulation requirement is very low as shown in Table 4.21 below. Only 4 corporations reported conforming to regulation requirements. Out of these 4, two have conformed to communication regulation while two have conformed to data protection act.

Table 4.21: Conformity to regulatory requirements

	Frequency	%
Communication	2	2.0
Data protection act	2	2.0
No Response	97	96
Total	101	100.0

Source: Author 2012

4.7.8 Satisfaction with research objectives

The respondents were also asked to state their satisfaction or dissatisfaction with the research objectives. The findings presented in Table 4.22 shows that more than 80 % are satisfied with the research objectives.

Table 4.22: Satisfaction with research objectives

	Yes		No	
	Frequency	%	Frequency	%
Satisfaction with research objectives	65	80.2	16	19.8

4.8 Summary

This chapter presented the findings of the study. The study found out that most state corporations have access control mechanisms and well defined access criteria. The corporations also conduct security awareness trainings, screen information security teams before employment and define authorities and responsibilities.

In terms of information security management, the state corporations have deployed different information security management tools such information security policy, business continuity plan and disaster recovery.

In addition, state corporations not only install anti-virus to protect their information from virus infections but also back up their critical data. Both the anti-virus and backup are updated with differing frequency. They also manage intrusion to organization data/information and prevent organization network from public network.

Furthermore, the state corporations have developed security infrastructure to manage data risk, respond and manage incidences, undertake information security awareness have internal policies and procedures to ensure information security and enforce and assess information security. However, conformity to regulation requirement is very low.

CHAPTER FIVE

SUMMARY, DISCUSSION, CONCLUSIONS AND RECOMMENDATIONS

5.1 Introduction

This chapter presents a summary of the findings, conclusions and the recommendations of the study. The study set out to establish the influence of Access Control on level of ISP; establish the extent to which Human Factors influence the level of ISP; to establish the extent to which use of Information Security Management Tools influences the level of ISP; to assess how Information Security Technology Usage influences the level of ISP. Further the study examined the extent to which availability of Security Infrastructure influences the level of ISP.

According to the above illustrated findings, the researcher observed that Access Control influences level of ISP. Human factors, Information Security Management Tools Usage, Information Security Technology usage and Availability of Infrastructure all are drivers of enhanced level of ISP within organizations.

Many reasons were advanced for increased number of security incidences within organizations. From the Ministry of Industrialization, related factors included intrusion by hostile agents, frequent Computer Viral attacks, information loss, identity theft, eFraud, Denial of service attacks, among others.

5.2 Summary of Findings

One five objectives of the study were: to establish whether access controls influence the level of ISP; to establish the extent to which human factors influence the level of ISP; to establish the extent to which use of information security management tools influences the level of ISP; to assess how information security technology usage influences the level of ISP and to establish the extent to which the availability of security infrastructure influences the level of ISP.

Most state corporations (75.2 %) have access control mechanisms. Similarly majority of state corporations also have well defined access criteria and can identify user of information (66.7

% and 67.7 % respectively). The most common types of access control mechanism are passwords and restricted access (57.0 % and 26.0 % respectively). Most state corporations (40.0 %) provide access based on the roles of the employees. Majority of state corporations (65.9 %) use passwords to authenticate the person accessing the information.

Human factor determinants for ISP by the state corporations are conducting security awareness trainings (34.7 %), screening of information security teams before employment (15.8 %) and authorities and responsibilities defined (62.4 %). Competence of security teams' members in the state corporations is mostly ensured through training (64.7 %).

The different information security management tools employed by the state corporations are security policy (36.0 %), business continuity plan (20.8 %), and disaster recovery plan (29.7 %).

Majority of state corporations (89.1 %) have installed anti-virus to protect their information from virus infections. Equally, 83.2 % have backed up their critical data. Close to half of the state corporations (47.5 %) reported updating anti-virus daily. 19.8 % update anti-virus automatically while 9.9 % update anti-virus weekly. In terms of data backup, 46.9 % of state corporations reported backing up their data daily while 16.3 % back up their data weekly. The most common approach of managing intrusion to organization data/information is restricted access (33.7 %) followed by firewall (13.7 %). Majority of state corporations prevent their network from public network through firewall (65.2 %). An addition 8.7 % use ISP to prevent their network from public network.

Data risk is mostly managed through backups (41.1 %). The most common incident response and management mechanism used is reporting to help desk (26.0 %). More than half of state corporations (55.7 %) undertake information security awareness based on necessity. Internal policies and procedures to ensure information security are present in close to 90 % of the state corporations. The most common mechanisms employed by corporations to enforce and assess information security is development of policies and procedures (55.9 %) followed by development of regulations/laws to govern information security (19.3 %). 12.9 % reported that the information security deployed is effective while 53.5 % have experienced information security breach. The above-mentioned issues may be related to the inadequate

budget allocated to the implementation of information security as shown below – only 13.8 % of the corporations have adequate budget. Conformity to regulation requirement is very low.

5.3 Discussion

As presented in Auerbach publications (2011), deployment of access control mechanisms and verification of the identity of a user (authentication) before full access to resource is granted are important to successful implementation of access control. This study established that most state corporations have access control mechanisms to ensure information security. Majority of state corporations also have well defined access criteria and can identify user of information. These are aimed at limiting information access and disclosure to authorized users as defined by Miller (2006). Information access is provided based on the roles of the employees and passwords are used to authenticate the person accessing the information. These findings draw a parallel to Lock's (2010) proposition that identity management has the most obvious direct connection to securing Information Systems operations and services.

Garry (2003) stated that safety-critical systems are designed, developed, tested, operated and maintained with human safety very much in mind. This study found out that human factor determinants for ISPD by the state corporations include conducting security awareness trainings, screening of information security teams before employment and authorities and responsibilities defined. These are aimed at minimizing human flaws that Hinson (2003) argues are the product of human errors. In addition, competence of security teams' members in the state corporations is ensured through training. Competent personnel are important for information security because as stated by Krause (1993), the practice of information security has become much more complicated and the need for qualified information security professionals has become critical.

The study found out that the state corporations have data risk management systems. A study by Nicasro (2011) found out that increasing amounts of sensitive corporate data are being held outside of central storage platforms, for example on laptops and mobile devices. The state corporations reported several medium of back up for their information (*see Table 4.12*). Another study by Moore (1993) established that the four most frequently indicated technologies used were anti-virus software, data back-up systems, system access controls, and encryption and this study the organizations have developed information security

management tools such as security policy, business continuity plan and disaster recovery plan.

Information security awareness as a necessity is common in the state corporations. Internal policies and procedures to ensure information security are also present in close to 90 percent of the state corporations (*Table 4.18*). These findings correspond somewhat to the findings by CIO East Africa (January 2011) that the most commonly used information system management tool is data recovery procedures, followed by information security policy. The common mechanisms employed by corporations to enforce and assess information security are development of policies and procedures and development of regulations/laws to govern information security. However, effectiveness of the information security deployed is very low (*Table 4.20*) and more than half have experienced information security breach. The above-mentioned issues may be related to the inadequate budget allocated to the implementation of information security as reported by most organizations. In addition, conformity to regulation requirement is very low and according to Lock (2010), drivers such as compliance with regulatory pressures, minimizing financial risks, securing corporate data and protecting a company's brand are all important aspects.

5.4 Conclusion

Information security is core to organizations operations. By definition who accesses what kind of organization's information, the organizations are able to ensure that only appropriate information is accessed by appropriate people. Government and its departments also have information that is not accessible to everybody and this information requires security.

State corporations, following the businesses model operate in an environment with increasingly powerful ways of manipulating and storing information. This is matched by growing threats to that information. Businesses need to manage their information so that they get the best value from it, and minimise the risks of losing it.

ISO/IEC 27001 standard defines the various ISPs that organizations should implement. The practices guide organizations on the types of controls, objectives and procedures that comprise an effective IT security program. This study established that access control, human factors, use of information security management tools, information security technology usage

and availability of security infrastructure all influence the level of ISP in government corporations.

According to a publication by Georgia Technology Authority (2008), each organization has the responsibility to exercise due diligence and due care in support of the organization's commitment to protecting its information assets, as well as for compliance with state regulatory requirements.

5.5 Recommendations

Based on the findings of this study, it is evident that access control, human factors, use of information security management tools, information security technology usage and availability of security infrastructure all influence the level of ISP in government corporations.

However, there is need for improvement in certain areas such as screening of information security teams before employment, development of information security policy, development and implementation of both business continuity plan and disaster recovery plan, adequate budget to implement information security and conformity to regulatory requirements.

5.6 Suggestions for Further Research

This study gave attention to the factors that influence the level of ISP in State Corporations in Kenya. The study could not exhaustively cover all these factors that influence the level of ISP in all State Corporations. There is therefore need for more research in this area.

The study recommends the utilization of a large study sample covering all State Corporations and Government Ministries enhance an in depth analysis and understanding their influence on the level of ISP; as well as on the areas that the study did not research on due to time constraints as well as limited resources.

There is need for further research to examine the relationship between different factors influencing level of Information Security and the number and frequency of security incidences experienced by the implementing organizations. The understanding of the factors employed by organizations will facilitate the formulation and adoption of integrated and comprehensive approach to ISP.

REFERENCES

- Cate F.H. (2008)** Information Security Breaches: Looking Back and Thinking Ahead.
- CIO East Africa (Dec 2010)** Information & Communication Technology magazine.
- Dubin J. (2006)** Access Management Solutions
- Davis F.D. (1993)** User Acceptance of Information Technology: Theories and Models.
- Daily Nation Newspaper, 14th October 2010**
- DOD website:** <http://www.mod.go.ke>
- Felicia (2011)** IADIS Information Systems.
- Fraenkel J.R. & Wallen N.E. (2008)** How to design and evaluate research in Education, Seventh edition. New York, McGraw-Hill.
- Gall M.D., Borg W.R. and Gall J.P. (1996)** External Validity – Educational Research
- Gary H. (2003)** Human Factors in Information Security
- Georgia Technology Authority (2008)** Information Security Infrastructure
- GISS (2011)** Respected – but still restrained
- Harry W. (2010)** Information Systems Security
- Hartwick and Barki (1994)** Challenges of Information Technology Management
- Hinson G. (2003)** Human Factors in Information Security

[Http://www.administrationpolice.go.ke](http://www.administrationpolice.go.ke) - Administration Police

[Https://www.cia.gov](https://www.cia.gov) CIA world factbook.

[Http://www.infosec.co.uk](http://www.infosec.co.uk) - 360 InfoSec 2010

[Http://www.kenya.go.ke](http://www.kenya.go.ke) - Kenya Government Portal

[Http://www.statehousekenya.go.ke](http://www.statehousekenya.go.ke) - State House Kenya

[Http://www.treasury.go.ke](http://www.treasury.go.ke) - The Treasury

Information Commissioner (2011) Achieving the value of being a model of best practice

ISO/IEC 27001 (2005) Information Technology – Security Techniques – Information Security Management Systems - Requirements

Johana M. (1993) Capturing Intentional and Rhetorical Information

Julie J.C. (2001) Information Security Tools and Practices.

Kevin P. (2003) Human Factors in Computing Systems.

Kothari C.R. (2003) Research Methodology (2nd Ed.). New Delhi. K K Gupta of New Age International (P) Ltd.

Martin L.N. (2009) Managing Information Security.

Mathieson K. (1991) Predicting User Intentions: Comparing the Technology Acceptance Model with the Theory of Planned Behaviour

Miller F. (2006) Reducing adverse outcomes.

Mugenda Olive .M. and Mugenda A.G. (1999) Research Methods, Quantitative and Qualitative Approaches. Nairobi. Act Press.

Nachmias and Nachmias (1976) Research Methods in the Social Sciences.

Ndungu C. (2004) Framework for Information Systems Audit: a case of Kenya Bureau of Standards

Peter A.T. (2001) Understanding Information Technology Usage: A Test of Competing Models

Renthia K. (May 2011) Investigative Africa: The effect of cyber crime to emerging economies

Ryan H. (2001) Information Security Practices & Experiences in Small Business.

Security Infrastructure Summary (2008) USF Journal

Steve R. (Dec. 2010) Information Security Journal.

Swanson M. & Guttman B. (1996) Generally Accepted Principles & Practices for Securing Information Technology Systems:

Swanson and Guttman (1996) Generally Accepted Principles and Practice for Securing Information Technology Systems

APPENDIX I: LETTER OF TRANSMITTAL AND INFORMED CONSENT

UNIVERSITY OF NAIROBI

Okoth Washington Oduor

University of Nairobi

Dept. of Extra Mural Studies

11th May 2011

Dear Sir/Madam,

RE: TO WHOM IT MAY CONCERN

I represent the University of Nairobi in the capacity of student researcher. My names are Okoth Washington Oduor; registration number is L50/76906/2009. Kindly grant access within your noble institution as your organization has been pre-selected to be included within my research scope. Data will be collected in the form of interviews, questionnaires and customer observations. Activity plan will be communicated adequately so that normal business will not be interrupted abruptly.

I would crave your indulgence in according me the needed cooperation as we go through the structured questionnaire and will ensure that all information received will be treated in full confidence, also will share prime findings of this research with your institution.

Many thanks in advance.

Okoth Washington Oduor

APPENDIX II: SURVEY QUESTIONNAIRE – STATE CORPORATIONS

UNIVERSITY OF NAIROBI

General instructions

Its is essential that every question be answered completely with a high degree of accuracy with details provided where necessary by ticking or marking X as deem appropriate.

Eligibility: Only state corporations within the ministry of Industrialization are required to participate.

Serial # (To be filled by Interviewer).....

Date:

Mode of survey Face –to – face interview () Mail survey () Email ()

PART A

General information of respondent

1. Organization _____
2. Position in the organization _____
3. Age bracket 18-30 () 31 – 40 () 41 – 50 () above 50yrs ()
4. Information security role _____

PART B

SECTION I

To establish whether access control influence the level of information security practice

1. Does your organization have access control mechanism? Yes () No ()
2. If the answer to the above question is Yes kindly state the access control mechanisms

3. Are access criteria defined in your organization? Yes () No ()
4. If the answer to the above question is Yes kindly state the access control mechanisms

5. Are users of information identified before access is granted? Yes () No ()
6. What methods of authentication do you use? _____

SECTION II

To establish the extent to which human factors influence the level of information security practice.

1. Has security awareness training been conducted to staff? Yes () No ()
2. Do information security teams undergo screening before employment or during employment? Yes () No ()

3. What mechanisms are put in place to ensure security team members are competent?

4. Are authorities and responsibilities defined for information security personnel?

5. Yes () No ()

SECTION III

To establish the extent to which use of information security management tools influence the level of information security practice.

1. Does the organization have an information security policy? Yes () No ()

2. Has Business Continuity Plan been developed and implemented in the organization?

3. Yes () No ()

4. Has Disaster Recovery Plan been developed and implemented in the organization?

5. Yes () No ()

6. Has any / both the BCP/DRP been tested for reliability? Yes () No ()

SECTION IV

To assess how information security technology usage influences the level of information security practice.

1. Does the organization have antivirus software installed? Yes () No ()

2. If the answer to the above question is Yes kindly state the frequency of update

3. Is critical data/information backed up? Yes () No ()

4. If the answer to the above question is Yes kindly state the frequency_____ and Medium_____

5. How is intrusion to organization data/information managed, detected or prevented?

6. _____

7. How is the organization's network protected from the public network?

SECTION V

To establish the extent to which the availability of security infrastructure influences the level of information security practice

1. How is information/data risk managed within the organization?

2. How is incident responded to and managed?

3. How often is staff given information security awareness?

4. Does the organization have internal policies and procedures? Yes () No ()

5. How is information security enforced and assessed? _____

SECTION VI

General comments

1. Do you believe that information security practice deployed by your organization is adequate/effective? Yes () No ()
2. Have you experienced any information security breach in the past? Yes () No ()
3. If the answer to the above question is Yes, kindly state:
4. Magnitude _____
5. Impact _____
6. Root cause _____
7. Corrective action _____
8. Duration of interruption _____
9. Do you have adequate budget to implement effective information security practice?
10. Yes () No ()
11. What are the regulatory/statutory requirements which your organization is complying/conforming to? _____

12. Are you satisfied with my research objectives?
13. Questions for researcher?

Thank you for filling this questionnaire