FACTORS AFFECTING CYBER SECURITY IN NATIONAL GOVERNMENT MINISTRIES IN KENYA

BY

SAMUEL WAITHAKA

D61/71991/2014

A RESEARCH PROJECT SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENT FOR THE AWARD OF THE DEGREE OF MASTER OF BUSINESS ADMINISTRATION, MANAGEMENT OF INFORMATION SYSTEMS, SCHOOL OF BUSINESS,

UNIVERSITY OF NAIROBI

OCTOBER, 2016

DECLARATION

This research project is my original work and it has not been presented for any course in any learning institution. All the sources used herein are duly acknowledged.

Signature……...…….…… Date……

SAMUEL WAITHAKA **Reg. No. D61/71991/2014**

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

Dr. Muranga Njihia **…….…….…….**

Signature……...…….…… Date……

ACKNOWLEDGEMENT

I must admit humbly that the success of this research has been largely due to collaborative efforts and devotion of many people to whom I owe a lot of gratitude. I would like to express my deepest appreciation to the following for their support that made this work a success.

I am sincerely grateful to God for the gift of serenity throughout my studies from the beginning of the course to its completion. I honour Thee for such a great accomplishment in my life.

To my project paper Supervisor, Dr. James Njihia for his great contribution and support offered that enabled this research project to take its present form, without his guidance and persistent help, this research would not have been successfully completed. Thankful to the Department of Management Science; School of Business for the facilitation in undertaking of my post graduate studies.

To my nuclear family members, extended Gathenji's family members and close friends who we had to forfeit shared social activities as I dedicated extra hours and days in accomplishing my studies.

Thank you to you all.

DEDICATION

This work is dedicated to the Gathenji's Family, who's besides my grandfather having no formal education, ensured all 1st generation members irrespective of gender, completed basic education. The 1st generation have fought to keep the baton on the race and pushed on the agenda of essential education for all within the family. The 2nd generation, who have been great beneficiaries of the spirit, are now much more than obliged to carry on the agenda to the next generation. This spirit has been my motivation in my post graduate studies and I'm willing to carry it on.

ABSTRACT

The main justification of e-government systems is to offer public services conveniently and continuously over open and distributed networks. Security reliability of information connected over distributed networks offering convenience to stakeholders is vital not only in the private sector but also in the public sector. The main aim of the study was to establish what factors affect cyber security in public service in Kenya, specifically National Government Ministries in Kenya. This study employed a descriptive research design. The target respondents for this study comprised of Information Communication Technology (ICT) Officers in the Ministries and Internal Auditors involved in review of Information Systems. The study collected primary data as the preferred source of research data with the help of structured questionnaires. This study concludes that factors affecting cyber security in the National Government Ministries in Kenya are principally divided in to external motivations for cyber attacks and internal organizational system vulnerabilities. The key external motivations for cyber attacks are i) systems sabotage and exploitation of systems' weakness, ii) business rivalry systems exploitation for illegal competitive strategy insights, and iii) systems attacks due to ideological differences. The internal organizational factors affecting cyber security were identified as i) lack of management support in implementation and adherence of cyber security strategy and standards, and ii) employees' systems exploitation for personal gains. Lack of management support in implementation of cyber security is a major contributor to poor cyber security in the Public Service. The sustained efforts for adoption of e-government across ministries service delivery should also propagate for sustainable cyber security mechanisms in the strategies' development and adoption. The management need to comprehend the impact of cyber attacks on Ministries service delivery. Cyber security issues need to championed even to the political class, so as to positively influence funds apportionment and drive for adherence to the cyber security strategy. There is also need to address the ethical aspect of employees working in the ministries' information systems in view of their involvement in systems sabotage and exploitation of the systems for financial gains.

TABLE OF CONTENT

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

CIS	:	Computer and Information Security
COMESA	:	Common Market for Eastern and Southern Africa
ICT	:	Information and Communication Technology
IFMIS	:	Integrated Financial Management Information System
IGAD	:	Intergovernmental Authority on Development
IS	:	Information System
IT	:	Information Technology
ITU	:	International Telecommunication Union
SME	:	Small and Medium Enterprises
SPSS	:	Statistical Package for Social Scientists

CHAPTER ONE

INTRODUCTION

1.1. Background of the Study

Infiltration of an organization information system could have far reaching consequences especially in the current era of information edge strategy. An organization can loose its competitive advantage which could lead to it's extinction, loss of privacy data leading to law suits and litigations, and also loss of trusts by the entity's stakeholders (Gaudin, 2007). Governments, commercial organizations and individuals around the world have invested heavily in Information and Communications Technologies (ICT), implying the systems' security is of utmost importance. To achieve this, they deploy technical security measures, and develop security policies that specify the correct behavior of employees, consumers and citizens. A secure e-government information system guarantees performance of the system and not only enhances reliability, confidence and belief, but also meets the security standards. A secure and reliable information system is recognized as a basis of enhancing confidence of e-government systems (Herath & Rao, 2009).

Recent development and adoption of financial institutions in Kenya of online and mobile banking services is leading organizations and individuals to previously unchartered risk levels and wider exposure. The government has introduced a number of ICT projects and some are now offered online; e.g. e-citizen, i-tax, Kentrade single window system, integrated financial management information system (IFMIS). Availability of government services through e-government besides offering convince to legitimate stakeholders, has also opened critical databases and infrastructure to the risk of cyber attacks (Tassabehji et al. 2007). Infiltration of e-government systems could have an impact on e-government users' systems' confidence and adoption (Ebrahim &

Irani 2005). Recently multiple public institutions have been targets of cyber insecurity; 103 government organizations were victim of cyber attacks in Kenya in the month of February 2012 as per the report by Serianu - IT security consulting firm. This paper evaluates factors affecting cyber security in Kenya with a bias towards the Public Service.

1.1.1 Cyber Security

Cyber security is basically the process of ensuring the safety of cyberspace from known and unknown threats. The International Telecommunication Union states that cyber security is the collective application of strategies, security measures, plans, threats administration tactics, engagements, training, paramount practices, assurance and expertize that can be used to guard the information system, organization and related assets (International Telecommunication Union, 2004). Cyber attack involves the malicious application of information and communication technology (ICT) either as a target or as a device by several malicious actors. Cyber security could also refer to the security of internet, computer networks, electronic systems and other devices (Olayemi, 2014) from the cyber attacks.

Cyber security has had enormous effects on businesses. The current information-age has increased the level of organizations dependency on cyberspace (Strassmann, 2009). Hacking of data and information leads to leakage on confidential data and information thereby negatively affecting organizations competitiveness (Tarimo, 2006). A successful attack compromises the confidentiality, integrity, and availability of an ICT system and the information it hampers in an organization (Bulgurcu et al., 2010). Cybertheft (cyber espionage) can result in exposure of economic, proprietary, or

confidential information from which the intruder can gain from while the legitimate organization losses revenue or patent information.

1.1.2 National Government Ministries in Kenya

Public offices are offices in the National Government, County Governments and other independent institutions where compensation and welfares of the office are payable straight from the Consolidated Fund or directly out of funds provided by the Kenyan legislature. A public service is a service which is provided by government to people living within its jurisdiction, either directly (through the public sector) or by funding delivery of services. These services are provided by various public offices in undertaking of their respective mandates. Recently there has been an increase of the public offices engaging and offering services to their users through the ICT infrastructure.

The National Government operates mainly through Ministries and parastatals which are established by the President through an executive order and currently there are twenty (20) Ministries in the National Government. Cabinet Secretaries are the Heads of Ministries and assisted by the Principal Secretaries and a team of technical areas employees to undertake the assigned mandate. While as the ministries and respective state departments undertake their mandate through the established team of respective core and support functions technical teams, the processes, controls and risk management are subject to review by the Auditor General as per Article 226 (3) of the Constitution of Kenya 2010. The Ministries are also subject to review by internal auditors who advise the management on the risk exposer and recommend correction measurers preferably prior to external audit review. While the external audit responsibilities do include the responsibility to assess security as part of certain

engagements, the final financial statements audits do not usually include the responsibility to assess cyber security. However, the internal audit IT audit function frequently includes the responsibility to assess cyber security, thus internal auditors are a reliable source of cyber security in ministries.

1.2. Problem Statement

The main justification of e-government systems is to offer public services conveniently and continuously over open and distributed networks. Security reliability of information connected over distributed networks offering convenience to stakeholders is vital not only in the private sector but also in the public sector, however for the public division there is different emphasis (Alfawaz, 2008). An effective information system including e-government systems incorporates personnel, infrastructure, processes and technologies (Alfawaz, 2008). This implies success of e-government systems is a factor of population social features of the country it is being implemented.

According to Serianu (2015), the public sector (government and related parastatals) were ranked first on risk levels in cyber security. Cyber attacks in government ministries in 2014 caused panic across the country since the intruders had penetrated websites expected to have state secrets, and sensitive security and financial information (Misiko, 2014). They include websites operated by the government's banker (CBK), Registration of Persons and Immigration Department, the government's financial accounting system (IFMIS), Attorney General's office and Kenya Defense Forces (Misiko, 2014). According to Serianu (2015), the public sector in Kenya lost more than Ksh5 billion from cybercrime attacks, this is besides the systems recovery costs. Cyber attacks impairs stakeholders' confidence of e-government's initiatives which thus hinders service delivery by the public sector hence the need for the study for factors affecting cyber security in public service.

Previous researchers have shown inter-relationship between e-government, organization administration and security issues (Dhillon and Backhouse, 2001; Dhillon and Torkzadeh, 2006; Heeks, 2003; 2006; Siponen and Oinas-Kukkonen, 2007; von Solms, 1999). Researchers have mainly concentrated on quantitative technical issues to address information systems' security (Siponen and Oinas-Kukkonen, 2007). However objective analysis of information systems' security indicates non-technical issues are essential as technical issues in protecting sensitive information (Dhillon and Torkzadeh, 2006; Siponen and Oinas-Kukkonen, 2007). Previous studies have mainly been undertaken in the developed countries context, implying there is limited open literature relating to dynamics such as environment, population awareness, socio culture for developing countries and how the aspects relate to standard approaches towards information system administration.

Operations in the public entities are different from the private entities operations hence the two necessitates different methods (Caudle, 1991; Fryer, 2007; Joia, 2003; Moon, 2000). The public entities are bound to open deliberations of their strategies, executive and legislative arms deliberations in their funds appropriations leading to political influence, provision of products for public good rather than economic viability and have to be geographically distributed over the administration region irrespective of the economic sense. This implies management of public entities have to align to their specific processes and the respective security models (Wimmer and von Bredow, 2001). Due to the nature of e-government requirement of openness, distribution and availability, e-government systems are a concern for privacy and security issues (Norris and Moon, 2005, Ebrahim and Irani, 2005, Wimmer and Bredow, 2001).

ICT and particularly e-government for developing countries and related cyber security in developing countries is generally under-represented in the open literature; there are

very few published empirical studies directly addressing the issue. Locally, Wechuli (2014) evaluated cyber security assessment framework in government Ministries in Kenya. The evaluation was on the limiting factors affecting the framework thus exploring on strategy and baseline assessment and prioritization (inventory of assets based of their importance in organizations infrastructure). This research is fairly related to this research as it evaluated the public service though it evaluated the cyber security strategy. This research will evaluate the cyber security in public service with additional factors especially in human and leadership who are the implementers of the framework and still have behavior management incorporated in their administration.

Wekundah (2015) did a study on the effects of cyber-crime on e-commerce for SMEs in Kenya. The study found out that most SMEs do not put emphasis or assign enough resources on cybercrime attack; they also lack expertise and experiences in handling cyber attack crimes. This study was done in the business sector and its findings may not be applicable in the government ministries.

Nyawanga (2015) studied the meeting the challenge of cyber threats in emerging electronic transaction technologies in Kenyan banking sector. The study found out that the cyber-crime rate has increased in the past 12 months with most 80 percent of attacks originating from China and Kenya itself. The study also found out that cyber-crime is mostly perpetrated by one of the bank staff knowingly or unknowing. Raising concerns for the need for cyber training for most if not all the banking staff. This study was done in the banking sector and its findings may not be applicable in the government ministries in Kenya.

The literature review indicates there is a differentiation between the private and the public sectors hence they required different approaches. Previous cyber security studies

were in different context from the Kenyan context while local studies looked at the cyber security framework in National Government Ministries in Kenya, but this study will expound further to incorporate the human and organizational factors affecting cyber security in the Ministries. The Public Service and more so the earlier established entities, the National Government Ministries have been victims of repeated cyber attacks besides the framework been in place. Thus the study addresses the question; what are the factors affecting cyber security in the National Government Ministries in Kenya?

1.3. Objectives of the Study

1.3.1 General objective

The main aim of the study was to establish what factors affect cyber security in public service in Kenya, specifically National Government Ministries in Kenya.

1.3.2 Specific Objectives

i. Establish the external motivations of cyber-attacks in National Government Ministries in Kenya.
ii. To determine internal organizational factors that may contribute to cyber security vulnerabilities in National Government Ministries in Kenya.

1.4. Value of the Study

The information generated in the course of this study would be important to policy makers since it would guide them when formulating policies and strategies affecting individual internet end users. This study provides information security professionals with relevant information that would be used to determine how to deal with cyber security threats.

The study would also contribute to cyber security research as it looks into deficiencies identified from the model analysis and provides improvement strategies against malicious insiders and outsiders. The insight would be useful to individuals employed in critical infrastructure areas as well as security agencies charged with protecting critical assets to assist them build or improve defenses against insider and outsider cyber threats. The information generated in the course of study would also enrich the body of knowledge on cybercrimes in the country and the Public Service.

To future researchers and academicians, the study would be important in the suggestion of areas requiring further research to build on the topic cyber security in public service in Kenya. In addition, the findings of this study would be important source of reference for future scholars and researchers.

CHAPTER TWO

LITERATURE REVIEW

2.1. Introduction

This chapter is about the review of literature relevant for the study. An overview of theoretical underpinning of the study, factors affecting cyber security in National Government Ministries in Kenya. It also presents empirical studies, summary of the literature review and research gap and the conceptual framework.

2.2. Theoretical Review of Cyber Security

This section discusses the theories on which the study is anchored. Specifically, the section discusses three theories: general deterrence theory; game theory; and the technology - organization - environment framework theory. These theories are discussed in details below:

2.2.1. General Deterrence Theory

This theory propositions that individuals can be discouraged from committing irregular selfish acts through the use of counter measures which include strong deterrents and sanctions comparative to the act (Schuessler, 2009). Counter measures such as education and training, back-ups, insurance and disaster recovery measures could be put in place to eliminate some threats or at least mitigate such risks (Schuessler, 2009).

This theory applies to cyber security through having a strong cyber defense relative to the IS strategic assets involved thus making an attack exceedingly difficult relative to returns. Successful attackers should also face severe retributions following their actions such that other aspirants may choose not to attack at all.

The theory relates to this study as it informs systems administrators and managers that a system defense should be relative to associated assets such that the cost of it attack are also high thus a deterrent to cyber attacks.

2.2.2. Game Theory

Games theory describes multi-person decision scenarios as games where each player chooses actions which results in the best possible rewards for self, while anticipating the rational actions from other players (opponents). In the field of cyber security, game theory will capture the nature of cyber conflict where the attackers' decision strategy are closely related to those by the defender (system administrator) and vice versa. A key concept of the theory is the ability to examine the huge number of possible threat scenarios in cyber system (Hamilton, 2002).

This theory application to the study is the multi scenarios application of the theory which should guide the system administrators and managers resources allocation in the ever changing security threats in cyber space including in the Public Service

2.2.3. Technology -Organization -Environment Framework Theory

Technology - organization - environment framework theory was advanced by Tornazky and Fleisher (1990). The framework shows an organization adoption and implementation of technological inventions is influenced by; technological context i.e. internal and external technologies for either or both the processes and equipment that are relevant to the firm; organizational context i.e. the managerial structure, degree of formalization and centralization, human resources and linkages among employees and the characteristics and resources of the firm in size; the environmental context which include the firm's competitiveness, the regulatory environment, the structures and size of the industry and the macro-economic context.

The technological context comprises of the technologies that are important to organizations comprising of those that are in the market place as well as those are currently been used by organizations. The organizational context can be defined in regards of available resources needed to support innovation acceptance within organizations. This comprises of firm size and scope; formalization, centralization, firm complexity and inter-connectedness, current managerial structure and lastly quality as well as the availability of organizational human resources. The environmental context characterizes firm setting whereby business is conducted. This is however influenced by the industry and competitors, the ability of firm's to access resources which are supplied by other organizations and lastly the made interactions with ruling governments.

Application of this theory to this study is on the impact of the environment on technology available for the cyber attacks and cyber security, competitors and regulation reaction and the management structure on the levels of cyber security in National Government Ministries in Kenya.

2.3. Factors Affecting Cyber Security

According to Serianu cyber security report 2015, the public sector (government and related parastals) were ranked first on risk levels. Effects of cyber security failure leads to the loss of intellectual property, direct financial loss from cybercrime, loss of sensitive business information (such as negotiating strategies), sabotage of operations, extra costs for systems' recovery, stakeholders loss of system' confidence, loss of competitive advantage as privileged information is availed to competitors and exposure of operations strategies which may cumulatively lead to loss of jobs or even extinction of an organization. Other costs include additional cost of securing networks and expenditures to recover from cyber attacks, reputational damage to the hacked

company. According to Serianu (2015), the public sector in Kenya lost more than Kenya Shillings 5 billion from cybercrime attacks, followed by the financial services sector at Kenya Shillings 4 billion.

Developing countries governments are now a days expected to be more transparent, share information with the public and educate the population on recent public developments and are therefore investing heavily in e-government (Kaisara and Pather, 2009). Unsecure e-governments systems will not only impair the convince of service delivery to citizens, but may lead to distorted information leading to stakeholders loss of system' confidence (SITA, 2002; Farelo and Morris,2006; Kaisara and Pather, 2009). E-government security is crucial for achieving an advanced stage of e-government services as it enhances trust and reliability of the service delivery. As the number of e-government services introduced to the users' increases, a higher level of e-government security is required. There is need to evaluate factors leading to effective cyber security in e-government services which could be different to the private sector as these two sectors operate in different environment and requirements.

Factors affecting cyber security can generally be divided in two groups; motivation or reasons for the attackers of the system, and system vulnerabilities or weakness exploited by the attackers for successful cyber attacks. The distinction mainly shows motivation factors are mainly external to the organization while systems' vulnerabilities are internal to the organization though the classification is not absolutely exclusive.

2.3.1 External Motivations of Cyber-Attacks

Availability of internet across the globe enhances convenience for legitimate users but it also avails critical assets and infrastructure to threat of cyber attack by illegitimate users. Recently there have been trends where the global internet is applied by state

agencies as a weapon against opponents including other states (Cornish, 2009). The activities of the illegitimate users can be organized in four major levels mainly based on the intention of the system attackers. The four levels are; hacking exploitation; serious and organized crime; ideological and political extremism; and state sponsored cyber-aggression.

Cyber attacks are motivated by various interests which usually vary but not exclusive for different groups. Motivations for economic issues may be different from political or national security matters. Even where the cyber attacker gives a reason for cyber attack, the real reason and main objective of the attacker is obscured or hidden (Shakarian et al., 2013). Extremist groups are recently using the cyber space for recruitment of members, coordination of physical attacks, sourcing of funds, attacking websites and spreading the group's propaganda (Gandhi et al., 2011). Financial gain is a major motivation for non-political systems attack (Andreasson, 2011).

Cornish (2009) on a paper on cyber security and politically, socially and religiously motivated cyber attacks evaluates the sources and nature of cyber attacks and denotes classifying and ranking various sources of cyber attacks is key and among the first steps in ensuring effective cyber security. The key motivations for cyber attackers need to be evaluated relative to an organizations systems for effective cyber security planning and implementation.

2.3.2 Internal Organizational Factors Affecting Cyber Security

There has been an omission of incorporation of human and organizational aspects in information systems security and mainly focusing on technological issues to address system's vulnerabilities and related cyber attacks (Dhillon and Backhouse, 2001). Organizational and human features are essential in protecting critical systems as there

is always an inter-link of these components with systems and technologies (Rasmussen, 1994; Reason, 1997). Previous studies found that management involvement, presence of security policy (Kankanhalli et al, 2003), and staff training and awareness (Bulgurcu, Cavusoglu & Benbasat, 2010) influence the effectiveness of ICT security in an organization. Governmental organizations are equally increasing their dependence to IS. For economic, social stability and to enjoy global competitiveness a government must have efficient, confidential and trustworthy information systems. Unsecure information systems of a public sector can negatively affect the trust and consequently the willingness of the public to seek services in governmental organizations which in turn can reverse economic and social stability (Tarimo, 2006).

Pelgrin (2014) in a study for positive change in cyber security strategy, human factor, and leadership identifies key factors to a successful cyber security as identifying the ICT assets and exposure involved, implementation and adherence of cyber security strategy and standards, enhancing responsiveness to frequent technological changes and threats arising there-off, human factor in addressing awareness and the arising vulnerabilities and lastly leadership as critical in sustainable cyber security as leaders are the drivers of the management policy. This research was on a global context and mainly on developed nations thus may be limited in application on developing nations and the public sector.

Cyber-attacks occasionally are instigated by insiders who can broadly be classified in three categories; i) organization employees retaliating their “unfair” treatment in the organization; ii) organization insiders exploiting the company’s assets for their self-interested gains; and iii) unintended cyber attackers insiders who are primarily not the

attackers but who unsuspectingly facilitate outside attacks (Andress & Winterfeld, 2011).

2.4. Empirical Studies

Studies of organizational and human factors affecting computer and information security (CIS) have evaluated various dimensions. The dimensions covered in the research include adoption and implementation of computer and information security strategy and policies, employees' acceptance and adherence to security policies and the impact of management support in adoption and implementation of CIS strategy and policies (Fulford and Doherty, 2003; Pahnila et al., 2007; Karyda et al., 2005). Culture in security systems is multidimensional and include reliable security processes, security governance, coordination and control (Ruighaver et al., 2007), top management backing (Knapp et al., 2006), employee involvement and training (Kraemer and Carayon, 2005), and employees' appreciation of security (Siponen, 2000). The impact of organizational and human features on information systems' security have also been researched (Werlinger et al., 2009). The above studies lead to a development of an integrated framework combining technological factors with organizational and human factors in information system security and also emphasizing on their interplay.

Ibikunle and Eweniyi (2013) did a study on challenges and solution to cyber security issues in Nigeria. The study recognizes objectives of cyber-security to include: addressing ICT systems and networks vulnerabilities; development and nurturing a cyber security culture by institutions and individuals; deriving an effective collaboration in cyber security between private and public organizations even beyond political bounders; keeping in-touch with new developments in cyber crime and their

effective solutions; and ensuring systems availability, confidentiality, integrity and authenticity.

Hussein and Khalid (2016) conducted a survey of cloud computing security challenges and solutions through review of existing literature. The study proposed model for cloud computing security which compose of three layers. In the first layer user's identification can be checked through proper authentication techniques. Security in the second layer depends on data identification and encryption. At the last layer cryptography technique is used to secure the transmission of the data.

Deshpande and Sambhe (2014) conducted a review of cyber security by looking at the strategy to security challenges. It identified latest issues on cyber security in India as including: cyber terrorism; use of internet in cyber terrorism, threat to ICT infrastructure, national cyber security and cyber security management. The findings indicate that many users value personal computers on security matters while ignoring security for mobile phones yet cyber attacks can be perpetrated using the phones and the consequences would be as severe just like attacks through personal computers. Personal firewalls can protect individual devices from attacks launched through the "air connection" or from the internet.

Deore and Waghmare (2016) carried out a literature review on cyber security automation for controlling distributed data. Most of the government and private organizations are trying to protect our data and information from cyber terrorist or hackers. Cyber security plays important role in information system as well as data sharing. For the protection of important information and data most of the software was developed by many organization using different techniques. Statistics indicate that data sharing was also challenge for government as private organization. Most of the

information was hacked at the time of sharing personal or government or official information. Different techniques were developed and used by scientist for the protection of information from attacker

Alfawaz (2008) on research on security of e-government systems in developing countries and identified key factors that impact on e-government security as top management support, staff and management security awareness, information system security infrastructure, security culture, management style, management change and security and privacy regulations. This paper is a key precursor of this study as is undertaken in the context of the public sector though not specific to Kenya.

Kyobe (2008) in research on Information Security challenges and their implications for emerging e-government structures in some African Countries denotes that information security is a major limitation caused not only by technological developments as normally perceived in literature, but also by political, cultural, legal and moral behaviours of the society. Further observation in the above paper notes, while the security challenges faced in e-government may not differ from those in the private sector, they are more complex and sensitive because e-government operations involve many citizens and are bound to various legal frameworks and requirements.

Research by Wechuli (2014) on cyber security assessment framework in government Ministries in Kenya evaluated the limiting factors affecting the framework thus exploring on strategy and baseline assessment and prioritization (inventory of assets based of their importance in organizations infrastructure). This research is fairly related to this research with additional factors especially in human and leadership who are the implementers of the framework and still have behavior management incorporated in their administration.

2.5. Summary of Literature Review and Research Gaps

Analysis of the literature available with relation to cyber security in the public sector shows it is critical for the public policy makers to know the impact of the interconnectivity through e-governments as initiatives as are layered onto existing systems. There is need for an inventory of critical infrastructure assets for a good cyber security strategy as an organization that does not know its assets cannot protect them. Knowing your Information Systems assets would also easily identify sources and nature of cyber threats thus plan adequately.

A system is strong as it weakest point thus the managers need to evaluate the organizational and human factors within it that can lead to cyber security vulnerabilities. These factors from prior literature review include; employees' cyber security awareness, management commitment to strategy and policies, organizational structure especially with Information Systems structure, skills and training of relevant implementers of cyber security and to some degree the ethical aspects of the organization employees.

There is very little information about challenges of information security in e-government more so in developing and East–African Countries' context. Previous studies on e-government have mainly focused on design, adoption and development process (Farelo & Morris, 2006:11; Kaisara and Pather, 2009). From the above literature review, there is very minimal done on factors affecting cyber security in Kenyan Public Sector and particularly the National Government Ministries thus creating a knowledge gap which this study wishes to address.

2.6. Conceptual Framework

According to Mugenda (2008), a conceptual framework is the researcher's own position on the problem and gives direction to the study. It may be an adaptation of a model used in a previous study, with modifications to suit the inquiry. Aside from showing the direction of the study, through the conceptual framework, the researcher can be able to show the relationships of the different constructs that he wants to investigate. The conceptual framework expresses the relationship between the independent and dependent variable is shown below.

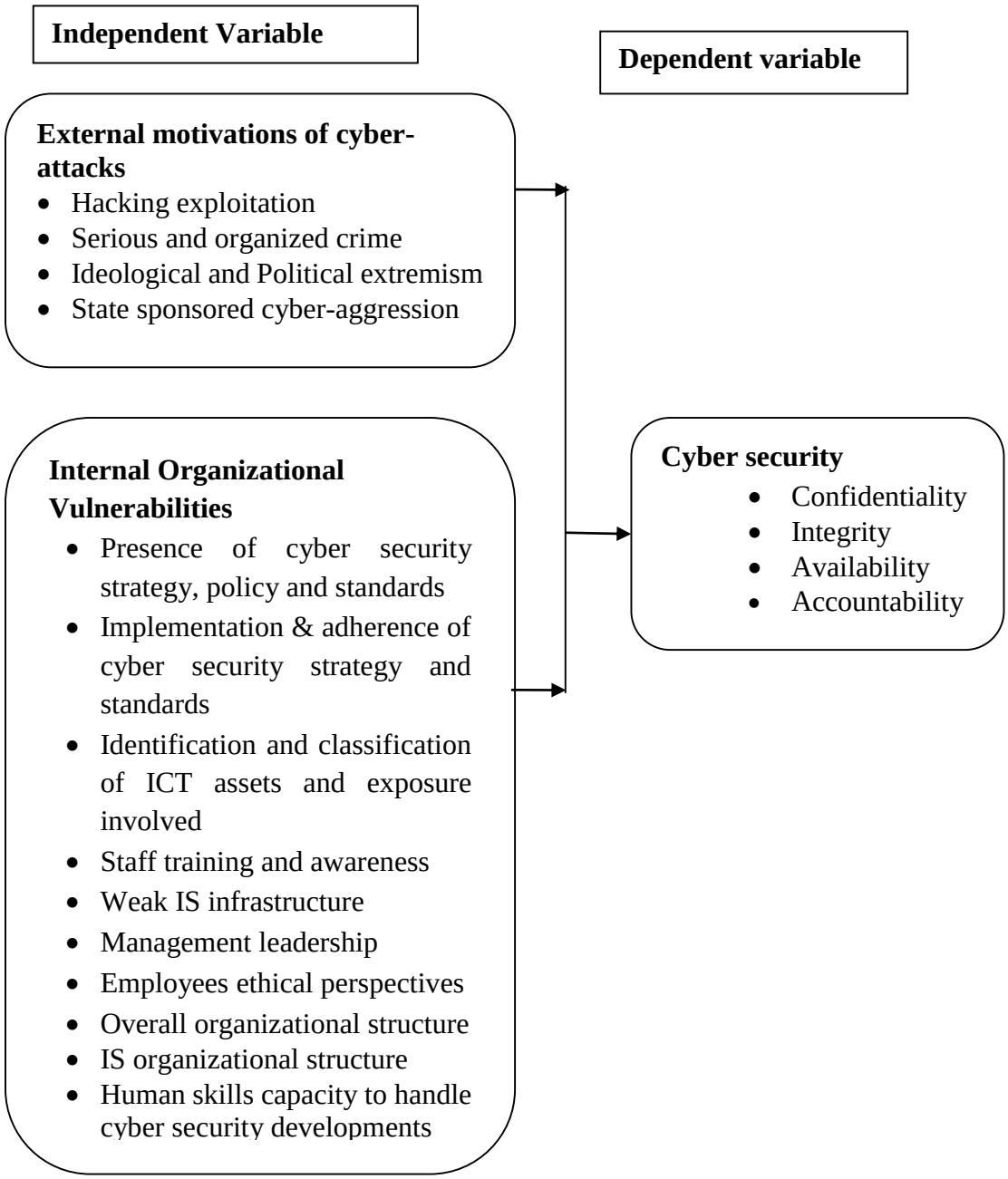

Figure 2. 2: Conceptual Framework.

CHAPTER THREE

RESEARCH METHODOLOGY

3.1 Introduction

This chapter outlines the research methodology that was applied in conducting this study. The chapter outlines the research design, target population, sample size and sampling procedures, data collection, research instruments and data analysis.

3.2 Research Design

This study employed a descriptive research design. This survey study was chosen as it is advantageous in demonstrating general conditions as presented by respondents. This type of descriptive research design determines and reports the way things are and in their ordinary setting. Descriptive research design is used where there is need for analysis of organizations, persons, settings or phenomena and reports the elements in their natural settings (Creswell, 2013). The design method have a set-up to maximize reliability and reduce biasness, thus giving a true picture of the elements under study (Creswell, 2013).

3.3 Population and Sampling

Population is defined as the total of individuals, elements, households or groups that are to be studied by the researcher (Cooper & Schindler, 2003). The target population of this study was all the National Government Ministries of Kenya as currently constituted which are twenty (20). Since the population is small a census was done. The target respondents for this study comprised of Information Communication Technology (ICT) Officers in the Ministries and Internal Auditors involved in review of Information Systems of all the 20 ministries of the National Government of Kenya where each ministry will pick 2 ICT officer and 2 Internal Auditors to enhance a ministry coverage

and presentation of factual information. Thus the total respondents for the study was 80.

3.4 Data collection

The study collected primary data as the preferred source of research data. This data was collected through the help of structured questionnaires which the researcher developed. The questionnaire contained closed ended and matrix questions so as to enhance the quality of obtained research data and easy of analysis for effective conclusions. The questionnaire was divided to three sections; general information which captured the respondents information and also the entity (Ministry) mandate and IS details, the external factors for main motivation of attack and finally the internal organization factors which captured the human and organizational aspects leading to systems vulnerabilities. The questionnaire covered the relevant study variables and adopted the five- point Likert scale to rate the respondents' agreement with each study variable.

The designed research instruments were distributed among the targeted respondents using the drop and pick later method, allowing the respondents one week so as to give the respondents ample time to fill in the questionnaires. At the point of dropping the questionnaire, the researcher obtained contact information from respondents so that any follow up will be done through the telephone.

3.5 Data Analysis Procedures

The completed returned questionnaires from the field were evaluated for consistency, cleaned, and then coded, entered and analyzed using the Statistical Package for Social Scientists (SPSS) Version 22.0 where the data analysis from the SPSS output were presented in tables, cross tabulation and charts.

Descriptive statistics was computed whereby means, frequencies and standard deviations were obtained. The study conducted factor analysis to establish the strength of factors affecting cyber security.

CHAPTER FOUR

DATA ANALYSIS, PRESENTATION AND INTERPRETATION

4.1 Introduction

This chapter presents the research findings on the basis of data collected from the field. Data was collected using questionnaires as the data collection instruments and summarized by use of descriptive statistics which involved the use of frequency tables, percentages, mean, standard deviation and factor analysis.

4.1.1 Response Rate

There were 55 respondents who returned the questionnaire out of the 80 questionnaire sampled and distributed implying a response rate of 69 percent. According to Mugenda and Mugenda (2003), a sample response rate of 60 percent and above is good. These finding is well illustrated in the Figure 4.1.

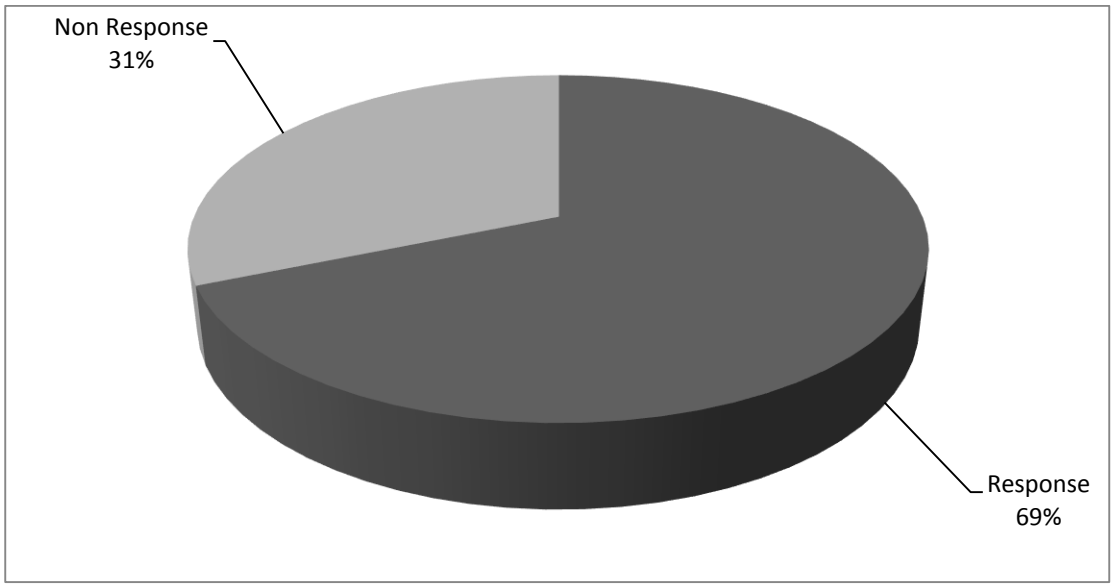

Figure 4.1: Response Rate

4.2 Demographic Information

The study sought to establish general information of the respondents as a way of fully understanding their suitability in undertaking the study. This general information is presented in the following subsections.

4.2.1 Cluster of Public Service

The respondents were required to indicate the cluster of public service their respective ministries belong. The findings are presented in Table 4.1.

Table 4.1: Cluster of Public Service

Sector	**Frequency**	**Percent**
Security	3	5.5
Public Administration & Social Services	22	40.0
Infrastructure	4	7.3
Education and Health	8	14.5
Productive Sector	18	32.7
Total	**55**	**100.0**

From the finding in Table 4.1, 5.5 percent of the respondents indicated security as their cluster in the public service, 40 percent indicated public administration and social services, 7.3 percent indicated infrastructure, 14.5 percent indicated education and health and 32.7 percent indicated productive sector. This finding implies that all clusters of the public service were involved thus the information provided were relevant and reliable for the study.

4.2.2 Gender Distribution

The respondents were asked to indicate their gender. The findings are shown in Figure 4.2.

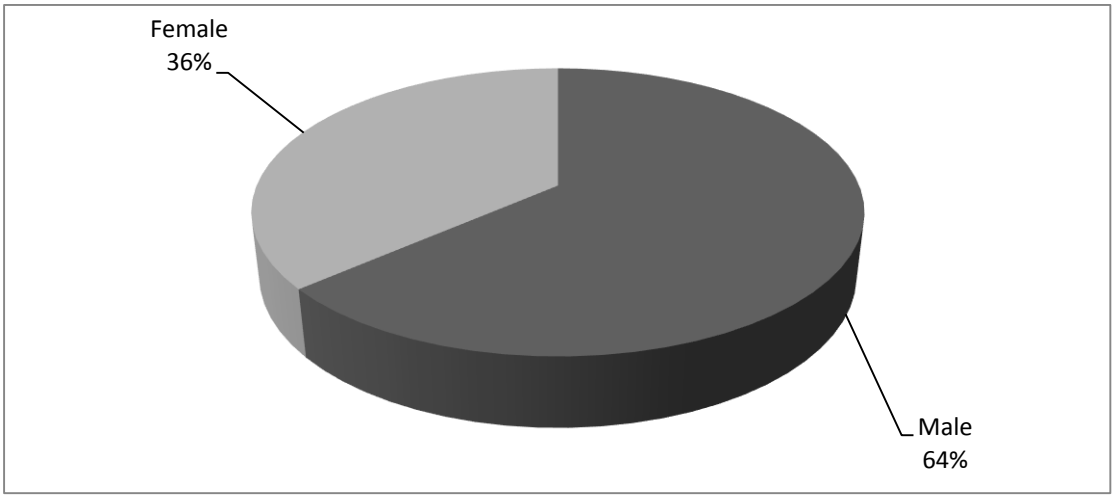

Figure 4.2: Gender Distribution

From the findings, 64 percent of the respondents were male while 36 percent were female. This shows that all gender were included thus provided a good representation for the study.

4.2.3 Highest Level of Education

The respondents were required to indicate their highest level of education. The findings are shown in Table 4.2.

Table 4.2: Highest Level of Education

	Frequency	**Percent**
Diploma	2	3.6
Bachelors	27	49.1
Masters	26	47.3
Total	**55**	**100.0**

From the findings on Table 4.2, 3.6 percent of the respondents indicated that they had diploma level of education level, 49.1 percent had bachelor's degree and 47.3 percent had master's degree. This implied that majority of the respondents had relevant knowledge on cyber security in public service in Kenya thus they had ease in addressing the question and provided the correct responses.

4.2.4 Management Level

The respondents were required to indicate their management level in their respective ministries. The finding is shown in Table 4.3.

Table 4.3: Management Level

	Frequency	Percent
Audit management	20	36.4
Audit staff	18	32.7
ICT Management	8	14.5
ICT Staff	9	16.4
Total	**55**	**100.0**

As indicated in Table 4.3, 36.4 percent of the respondents were in audit management, 32.7 percent were in audit staff, 14.5 percent were in ICT management and 16.4 percent were in ICT staff. This shows that the study covered across the management level in the ministries thus the information provided by the respondents were relevant for the study.

4.2.5 Work Experience

The respondents were requested to indicate their work experience at their respective ministries. The finding is presented in Table 4.4.

Table 4.4: Work Experience

Years Range	Frequency	Percent
Up to 5 years	4	7.3
5 – 10 years	18	32.7
10 – 15 years	16	29.1
15–20 years	11	20.0
Over 20 years	6	10.9
Total	**55**	**100.0**

From the finding in Table 4.4, 7.3 percent of the respondents had a work experience of up to 5 years, 32.7 percent had 5-10 years, 29.1 percent had 10-15 percent years, 20 percent had 15-20 years and 10.9 percent had over 20 years work experience. This shows that the respondents had worked long enough thus had clear understanding on the factors affecting cyber security in public service in Kenya, specifically National Government Ministries in Kenya thus provided reliable information for the study.

4.2.6 Cyber Attacks Targets

The respondents were asked to indicate what the previous cyber attacks were targeted to. The findings are shown in Table 4.5.

Table 4.5: Cyber Attacks Targets

	Frequency	Percent
Core functions	8	14.5
Support Functions	20	36.4
both core & support	13	23.6
none	14	25.5
Total	**55**	**100.0**

As shown in Table 4.5, 14.5 percent of the cyber attacks targeted core functions of the ministries, 36.4 percent targeted support functions, 23.6 percent targeted both core and support and 25.5 percent indicated none. The respondents responses indicates a trend where the support functions systems are more targeted for cyber attacks than core functions systems.

4.2.7 Organizational Structures Applied at the Ministries

The respondents were asked to indicate the type of organizational structure the Ministry's overall management and Information System management applies. The finding is presented in Table 4.6.

Table 4.6: Organizational Structures Applied at the Ministries

	Ministry Frequency	**Ministry Percent**	**IS Frequency**	**IS Organizational Percent**
Centralized	46	83.6	43	78.2
Decentralized	7	12.7	7	12.7
Matrix	2	3.6	5	9.1
Total	**55**	**100.0**	**55**	**100.00**

From the finding in Table 4.6, 83.6 percent of the respondents indicated that their ministries use centralized structure, 12.7 percent indicated decentralized and 3.6 percent indicated matrix structure. Further the respondents indicated that 78.2 percent IS management use centralized structure, 12.7 percent use decentralized and 9.1 percent use matrix structure The respondents indicates the dominant organizational structure in National Government Ministries both at the overall and the Information System management is centralized.

4.3 External Motivations of Cyber-Attacks

Several statements on external motivations of cyber attacks in organizations were identified and the respondents were required to indicate the extent to which they agree to each in respect to their ministry. A scale of 1-5 where, 1= no extent, 2= little extent, 3= moderate extent, 4= large extent, and 5= very large extent was used. From the findings mean, standard deviation and factor analysis were calculated for ease of interpretation and generalization of finding. The findings are shown on Table 4.7, 4.8 and 4.9.

Table 4.7: External Motivation / Drivers of Cyber-Attacks

	Var No.	**Mean**	**Std. Dev**
Organized crime aiming at Ministry's services sabotage	022	3.56	1.198
Hacking exploitation (people trying out their hacking skills for challenge and peer status)	017	3.27	1.339
Serious and organized crime for financial gain	019	3.20	1.223
Systems attack due to ideological and political differences	023	3.07	1.245
Serious and organized crime for industrial knowledge or intellectual property theft	021	2.81	1.248
Serious and organized crime for patent property theft	020	2.60	1.195

Former Public Service employees disgruntled by their dismissal	018	2.40	1.029
Inter-states (other States governments' initiatives) cyber aggression	024	2.29	1.314

The mean values of the finding range from 2.29-3.56 which shows that the respondents had mixed reactions on the responses which concurs with the finding of Kyobe (2008) who notes that information security is a major limitation caused not only by technological developments as normally perceived in literature, but also by political, cultural, legal and moral behaviors of the society.

The prominent external motivations for cyber attacks from the analysis were organized crime aiming at ministry's systems' sabotage, hacking exploitation and serious and organized crime for financial gain while inter-states cyber-aggression is the least likely source of cyber attacks for National Government Ministries in Kenya.

4.3.1 Factor Analysis of External Motivations for Cyber Attacks

Table 4.8 Total Variance Explained – External Motivations for Cyber Attacks

Component	Initial Eigenvalues			Rotation Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	6.145	76.818	76.818	2.924	36.549	36.549
2	.905	11.311	88.129	2.813	35.159	71.709
3	.359	4.486	92.615	1.672	20.906	92.615
4	.184	2.303	94.918			
5	.165	2.067	96.985			
6	.143	1.793	98.778			
7	.060	.755	99.533			
8	.037	.467	100.000			

There were 8 variables (statements) which were to enable us get key motivation or drivers of cyber attacks. Opting for 3 factors to explain the same, it showed the 3 components explained 92.615 percent of the total variation which is even better because

the rule of thumb is that 70 percent is always sufficient. Component 1 explained 36.549 percent, component 2 had 35.159 percent and component 3 had explained 20.906 percent respectively. This indicates the three derived components have each significant contribution to external motivation of cyber attacks ranging from 20.9 - 36.6 percent in National Government Ministries in Kenya.

Table 4.9 Rotated Component Matrix – external Motivations

Var No.		**Component**		
	Variable Statement	1	2	3
var022	Organized crime aiming at Ministry's services sabotage	.899		
var017	Hacking exploitation (people trying out their hacking skills for challenge and peer status)	.859		
var019	Serious and organized crime for financial gain	.694	.573	
var024	Inter-states (other States governments' initiatives) cyber aggression		.880	
var018	Former Public Service employees disgruntled by their dismissal		.879	
var021	Serious and organized crime for industrial knowledge or intellectual property theft	.516	.614	.535
var023	Systems attack due to ideological and political differences	.582		.729
var020	Serious and organized crime for patent property theft		.610	.675

The first factor or component could comprise of Var 022, var 017,var 019, var 021 and var 023. The second factor or component could comprise of Var 019, var 024, var 018, var 021 and var 020. The third factor or component could comprise of Var 023, var 020,

and var 021. Based on the prior variable statements and inter-relations as observed above, I would derive the three components as; i) systems sabotage and exploitation of systems' weakness, ii) business rivalry systems exploitation for illegal competitive strategy insights, and iii) systems attacks due to ideological differences.

4.4 Internal Organizational Factors Affecting Cyber Security

Several internal organizational factors that may contribute to cyber security vulnerability in organizations were identified and the respondents were required to indicate the extent these factors played a role of cyber security vulnerabilities at the Ministry. A scale of 1-5 where, 1= no extent, 2= little extent, 3= moderate extent, 4= large extent, and 5= very large extent was used. From the findings mean and standard deviation were calculated for ease of interpretation and generalization of finding. The findings are shown on Table 4.10

Table 4.10: Internal Organizational Factors Affecting Cyber Security

Variable Statement	**Var No.**	**Mean**	**Std. Dev**
Weak information infrastructure systems e.g. un-update systems patches	033	3.98	.804
Lack of audit (review) of the Ministry cyber security capacity and adherence	042	3.94	.950
Ministry's management lack of support for acquisition and development of Cyber security human skills (personnel)	041	3.87	.963

Poor implementation and adherence of cyber security strategy and standards by involved management	032	3.83	1.032
Ministry's management lack of provision of funds for sustainable cyber security systems	040	3.83	.995
Ministry's management not acting as key leader in implementation and adherence of cyber security strategy and standards	039	3.81	.924
Management understanding of implications of cyber attacks to the Ministry's IS affects cyber security implementation	043	3.78	.994
Employees non adherence to cyber security strategy and standards	035	3.72	.870
Employees poor cyber security awareness relative to ICT infrastructures, assets and exposures involved	036	3.68	.817
Lack of clear identification and classification of ICT assets and exposure involved	034	3.67	1.001
Ministry cyber security policy and standards deficiency	031	3.65	.927
Poor cyber security responsiveness in line with cyber threats / attacks due to overall organizational structure	037	3.60	1.011
Poor cyber security responsiveness in line with cyber threats / attacks due to IS organizational structure	038	3.54	.958

Lack of legislative penalties for cyber attacks implication e.g. privacy details exposure	044	3.49	1.016
Employees action derived for personal financial gains	028	3.40	1.285
Unintentional employees actions but leading to systems attack	030	3.21	.994
Lack of market / environment pressure to sustain a high level of cyber security	045	3.21	1.066
Disgruntled employees launching retaliatory attacks to sabotage systems / services delivery	029	3.10	1.030

The mean values for the finding ranges from 3.10-3.98 an indication that the questionnaire' statements were applicable to the respondents' information systems set-up thus consistent with Alfawaz (2008) findings who identifies keys factors that impact on e-government security as top management support, staff and management security awareness, information system security infrastructure, security culture, management style, management change and security and privacy regulations.

4.4.1 Factor Analysis on Internal Organizational Factors Affecting Cyber Security

The study carried out factor analysis to establish the strength of internal organizational factors affecting cyber security. The findings are shown below in Table 4.9

Table 4.11: Total Variance Explained Internal Organizational Factors

Component	Initial Eigenvalues			Rotation Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	15.359	85.327	85.327	9.674	53.744	53.744
2	1.373	7.630	92.957	6.415	35.641	89.384
3	.387	2.148	95.105	1.030	5.720	95.105
4	.269	1.495	96.600			
5	.131	.728	97.328			
6	.088	.490	97.818			
7	.076	.420	98.237			
8	.061	.337	98.574			
9	.056	.308	98.882			
10	.047	.259	99.142			
11	.029	.159	99.301			
12	.028	.155	99.455			
13	.025	.141	99.596			
14	.022	.123	99.719			
15	.017	.095	99.814			

16	.014	.077	99.891			
17	.011	.060	99.951			
18	.009	.049	100.000			

Applying the extraction method on the 18 principal component analysis with extraction of 3 components, the three derived components explained 95.105 percent of the total variation. Components 1 explained 36.549 percent, component 2 had 35.159 percent and component 3 had explained 20.906 percent respectively. Further the three derived components were subjected to rotated component matrix relative to earlier 18 variable statements. The results are as per table 4.12 below.

Table 4.12: Total Variance Explained Internal Vulnerabilities

Var No.	**Variable Statement**	**Component**		
		1	**2**	**3**
var032	Poor implementation and adherence of cyber security strategy and standards by involved management	.938		
var040	Ministry's management not acting as key leader in implementation and adherence of cyber security strategy and standards	.913		
var043	Management understanding of implications of cyber attacks to the Ministry's IS affects cyber security implementation	.899		
var039	Ministry's management not acting as key leader in implementation and adherence of cyber security strategy and standards	.861		

var042	Lack of audit (review) of the Ministry cyber security capacity and adherence	.855		
var033	Weak information infrastructure systems e.g. un-update systems patches	.854		
var034	Lack of clear identification and classification of ICT assets and exposure involved	.843		
var035	Employees non adherence to cyber security strategy & standards	.830	.528	
var031	Ministry cyber security policy and standards deficiency	.783	.588	
var041	Ministry's management lack of support for acquisition and development of Cyber security human skills (personnel)	.780		
var044	Lack of legislative penalties for cyber attacks implication e.g. privacy details exposure	.733	.646	
var028	Employees action derived for personal financial gains	.696	.541	
var036	Employees poor cyber security awareness relative to ICT infrastructures, assets and exposures involved	.685	.657	
var030	Unintentional employees actions but leading to systems attack		.920	
var029	Disgruntled employees launching retaliatory attacks to sabotage systems / services delivery		.912	
var045	Lack of market / environment pressure to sustain a high level of cyber security		.798	

var038	Poor cyber security responsiveness in line with cyber threats / attacks due to IS organizational structure		.777	
var037	Poor cyber security responsiveness in line with cyber threats / attacks due to overall organizational structure		.728	

The first factor or component comprise of Var 032, var 040, var 043, var 039, var 042, var 033, var 034, var 035, var 031, var 041, var 044, var 028 and var 036. The second factor or component comprise of var 030, var 029, var 045, var 038, var 037, var 036, var 044, var 031, var 028 and var 035. The third factor or component could comprise none of those variables so it's better if we just assumed it. Based on the prior statements and inter-relations observed above, I would derive the two components statements as; i) Management support in implementation and adherence of cyber security strategy and standards, and ii) Employees systems exploitation for personal gain

4.5 Discussion of Findings

This study was evaluating factors affection cyber security in the National Government Ministries in Kenya, and the first objective was external motivations of cyber attacks. Literature review showed there are four key motivations for cyber attacks i.e. hacking exploration, serious and organized crime, ideological and political extremism and state sponsored cyber aggression. Analysis of data on the for external motivations for cyber attacks shows three key motivations as i) systems sabotage and exploitation of systems' weakness, ii) business rivalry systems exploitation for illegal competitive strategy insights, and iii) systems attacks due to ideological differences. This shows the findings

of the literature review and of the study are quite inter-linked with the findings of the study indicating incorporation of the motives of the different systems attackers more explicitly. The findings also collaborate Pelgrin (2014) findings for positive change in cyber security strategy, human factor and leadership which noted identifying the ICT assets and exposure involved and enhancing responsiveness as per threats arising as technology changes as key to a successful cyber security.

The second objective of the study was to evaluate internal organizational factors affecting cyber security. The literature review identified a number of key organizational vulnerabilities including lack of cyber security strategy, policy and standards, poor implementation and adherence of the cyber security, lack of clear identification and classification of ICT assets and exposure involved, poor management leadership in cyber security and human skills capacity and awareness on current cyber security trends. This study has deduced the internal system vulnerabilities as i) lack of management support in implementation and adherence of cyber security strategy and standards, and ii) employees' systems exploitation for personal gains. Mainly the findings of literature review and of this study are similar only that's the study findings have lumped together the earlier reviewed literature review finds to two components.

The findings of the study on internal factors affecting cyber security collaborates with the findings of Kankanhalli et al (2003) and Bulburcu, Cavusoglu & Benbasat (2010) which found out that management involvement, presence of security policy and staff training and awareness influence the effectiveness of ICT security in organization. The findings also collaborate Pelgrin (2014) findings for positive change in cyber security strategy which noted key components as identifying the ICT assets and exposure involved, implementation and adherence of cyber security strategy and standards,

enhancing responsiveness to frequent technological changes and threats arising there-off, human factor in addressing awareness and the arising vulnerabilities and lastly leadership as critical in sustainable cyber security as leaders are the drivers of the management policy. The findings on employees exploitation of systems for unauthorized personal gain collaborates the findings of Andress & Winterfeld (2011) and the finds of Nyawanga (2015) on cyber threats in Kenyan banking sector which showed that cyber crime is mostly perpetrated by one of the entity's staff knowingly or unknowingly.

CHAPTER FIVE

SUMMARY, CONCLUSIONS AND RECOMMENDATIONS

5.1 Introduction

The chapter provides the summary of the findings and it also gives the conclusions and recommendations of the study based on the objectives of the study. The conclusions and recommendations drawn were focused on addressing the objective of this study.

5.2 Summary of the Findings

This study was evaluating factors affecting cyber security in the National Government Ministries in Kenya. The study identified external motivations for cyber attacks as i) systems sabotage and exploitation of system weaknesses, ii) systems attacks due the associated variable statements shows attempts to incapacitate ministries' systems personnel trying out their skills on ministries systems and attempt to get financial benefits to the organized groups and individuals. The systems attacks due to competitive edge is also quite associated with the first component of systems sabotage indicating external parties are evaluating public entities strategies and developing counter strategies. The second component as per associated variable statements include inter-states cyber aggression and former disgruntled employees indicating external agencies sourcing for intellectual property through unauthorized means. This would partially explain trends within this region (Africa and mainly COMESA countries including Tanzania) where key projects by the country are been replicated across the countries e.g. standard gauge railways, ports' enhancements, electricity generations projects and developments of blueprints for development are just replicated across the region.

The public entities agencies managers also need to be wary of private entities engaging in near similar functions or operates as interested parties either in sub-contracting of services, tenders as the trends indicates these entities would involve even former public servants to get privilege skills or even sabotage national government information systems to attain or retain competitive advantage in services or contracts offered by the national government agencies.

The third reason for external motivation for cyber attack was identified as iii) systems attacks due to ideological differences would partially be explained due to the recent developments where the country is involved in IGAD activities mainly in lawless Somalia. The country has experienced systems attacks mostly associated with Al-Shabab group where the Kenya Defense Forces twitter account and the Deputy President's twitter accounts with defacing messages mainly on Kenya's involvement in Somalia war.

The second objective of the study was to establish internal organizational factors affecting cyber security where two factors were identified i.e. i) Lack of management support in implementation and adherence of cyber security strategy and standards, and ii) employees' systems exploitation for personal gains. This study findings clearly collaborates with recent findings which observed that there is inter-play of human and organizational factors including Pelgrin (2014), Werlinger et al. (2009) and Alfawaz (2008) in cyber security effectiveness. The findings shows promoters of information systems in the Public Service only highlights the performance perspective while not highlighting the assets exposure involved in the convenience introduced by wide and open availability of the systems mainly to the public. The employees' ethical aspect of the systems users is also essential in the systems' administration and application and it

quite demonstrated by multiple cases and instances of malpractices in use of computerized systems in the region.

5.3 Conclusion

This study concludes that factors affecting cyber security in the National Government Ministries in Kenya are principally divided in to external motivations for cyber attacks and internal organizational system vulnerabilities. The key external motivations for cyber attacks are i) systems sabotage and exploitation of systems' weakness, ii) business rivalry systems exploitation for illegal competitive strategy insights, and iii) systems attacks due to ideological differences. While as the systems sabotage and ideological differences were expected to motivate cyber attacks in the National Government Ministries in Kenya, the systems attack due to illegal competitive strategy insights was unexpected considering that ordinarily Government entities are not involved in commercial products as its final product.

The internal organizational factors affecting cyber security were identified as i) lack of management support in implementation and adherence of cyber security strategy and standards, and ii) employees' systems exploitation for personal gains. Lack of management support in implementation of cyber security is a major contributor to poor cyber security in the Public Service.

The administrators and managers of e-governments needs to incorporate cyber security effectiveness across established systems as unsecure information systems can negatively affect the trust and consequently the willingness of the public to seek services in governmental organizations which in turn can reverse economic and social stability.

5.4 Recommendation

The sustained efforts for adoption of e-government across ministries service delivery should also propagate for sustainable cyber security mechanisms in the strategies' development and adoption. The management need to comprehend the impact of cyber attacks on Ministries service delivery. Cyber security issues need to championed even to the political class, so as to positively influence funds apportionment and drive for adherence to the cyber security strategy. The observation that the Public Service is also subject to competitive edge strategies illegal exploration including by inter-states agencies implying there is need to apply strategies similar to private-organization oriented mitigation measures to protect the country's intellectual properties and sustain its competitive advantage in the region.

There is also need to address the ethical aspect of employees working in the ministries' information systems in view of their involvement in systems sabotage and exploitation of the systems for financial gains. The General Deterrence Theory will be of use to the management where they would put in place measures that repercussions for systems exploitations are more costly than intended benefits, hence employees would not wish to be caught in the intrigues.

5.5 Limitation of the Study

The researcher encountered reluctance among target respondents in giving information. This is because the information needed was sensitive and it would indicates incompetency of the Information Communication Technology (ICT) practitioners hence the respondents feared they could be reprimanded by the management of the respective ministry. The researcher assured the respondents that the information

collected was only for research purpose and would not be a basis for management evaluation and the respondent's identity was confidential to the researcher.

A number of respondents were also of the view that internal employees' exploitation of information systems are not cyber-attacks. The researcher explained that cyber-attacks can be instigated by either internal or external parties as long as there is malicious exploitation of the information system for unauthorized use.

Another limitation was availability of ICT practitioners and auditors to fill the questionnaires owing to their busy schedule. The researcher addressed the limitation by dropping the questionnaires at the sampled employees offices and following up on them using emails, telephone calls and agreeing on the collection day.

5.6 Suggestion for Further Studies

The study sought to establish what factors affect cyber security in public service in Kenya, specifically National Government Ministries in Kenya. Other studies should be conducted in other sectors for comparison and generalization of findings.

Due to the dynamic nature of the ICT and the cyber-challenge and the ever dynamic and innovation of ICT products there is need to further study to determine the changes and the dynamic nature of cyber-crime in other state corporations.

Further studies can also explore on how to address external and internal factors affecting cyber security in the Public Service as identified in this study.

REFERENCES

Alfawaz, S, May, LJ & Mohanak, K 2008, 'E-government security in developing countries: a managerial conceptual framework', paper presented to International Research Society for Public Management Conference, Queensland University of Technology, Brisbane, 26-28 March 2008.

Bougaardt, G and Kyobe, M. "Investigating the Factors Inhibiting SMEs From Recognizing and Measuring Losses From Cyber Crime in South Africa" The Electronic Journal Information Systems Evaluation Volume 14 Issue 2 2011, (pp167-178),

Brenner, S., W. (2002b). The privacy privilege: Law enforcement, technology and the constitution. *Journal of Technology Law and Policy* 7 (2) 123-94.

Brenner, S.,W. (2002a) Organized crime? How cyberspace may affect the structure of criminal relationships. *North Carolina Law & Technology* 4 (1)

Brenner, S.,W. (2004). Toward a criminal law for cyberspace, Distributed Security. Boston University *Journal of Science & Technology Law* 10 (2).

Bulgurcu, B., Cavusoglu, H., &Benbasat, I. (2010). Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness,*MIS Quarterly*34(3), 523-548.

Chang and C-S. Lin (2007) "Exploring organizational culture forinformation security management," *Industrial Management & DataSystems*, vol. 107, no. 3, pp. 438-458.

Chau, P. Y., Kuan, K. K., & Liang, T. (2007). Research on IT value: What we Have Done in Asia and Europe. *European Journal of Information Systems*,*16*(3), 196.

Cooper, D. R., Schindler, P. S., & Sun, J. (2003). Business Research Methods.

Cooper, D.R., & Schindler, P.S. (2003). Business Research Methods. (8th ed.). Boston: 15 McGraw-Hill Irwin.

Creswell, J. W. (2013). *Qualitative inquiry and research design: Choosing among five approaches*. Sage.

Dacin, M. T., Goodstein, J., & Scott, W. R. (2002). Institutional Theory and institutional Change: Introduction to the Special Research Forum. *Academy of Management Journal*, *45*(1), 45-56.

Dhillon, G., &Torkzadeh, G. (2006). Value-focused Assessment of Information Systems Security in Organizations, *Information Systems Journal*16(3), 293-314.

Einhorn, H. J., & Hogarth, R. M. (1981). Behavioral Decision Theory: Processes of Judgment and Choice. *Journal of Accounting Research*, 1-31.

Glenny, M., Glick, B., & Wainwright, R. (2010). Cybercrime, cybersecurity and the future of the internet.

Herath, T., & Rao, H. R. (2009). Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organizations.*European Journal of Information Systems*18(2), 106-125.

Hulme, G. V. (2011). SCADA Insecurity-Stuxnet put the Spotlight on Critical Infrastructure Protection but Will Efforts to Improve it come too late?*Information Security Magazine*, 13(1), 38-44.

International Telecommunication Union (2004). Understanding Cybercrime: A Guide for Developing Country.

Jin, X. Q. Z. G. C. (2006). Theoretical Trace and Framework of Overall Innovation Management. *Chinese Journal of Management*, *2*, 002.

Kankanhallia, A., Teo, H., Tan, B., & Wei, K. (2003). An Integrative Study of Information Systems Security Effectiveness, *International Journal of Information Management* (23), 139-154.

Kimutai, J. K. (2014). *Social media and national security threats: a case study of Kenya* (Doctoral dissertation, University of Nairobi).

King'ori, P. M. (2014). *Assessment of Awareness and Preparedness of Cyber cafe Internet Users to deal with threats of cyber crimes: A case of Nairobi County* (Doctoral dissertation, University of Nairobi).

Kothari, C. R. (2004). *Research Methodology: Methods and Techniques*. New Age International.

Kyobe, M. (2008). Evaluating Information Security within SMEs engaged in E-commerce in South Africa. *Institute for Small Business & Entrepreneurship*, 5-7.

Magutu, P.A., Ondimu, G.M., &Ipu, C.J. (2011) Effects of Cybercrime on State Security: Types, Impact and Mitigations with the Fiber Optic Deployment in Kenya, *Journal of Information Assurance & Cyber security*.

Misiko H (2014, July 30). How Anonymous and other Hackitivists are waging war on Kenya. The Washington Post. Retrieved from Http://washingtonpost.com/news/worldviews/wp/2014/07/30.

Mugenda, A. G. (2008). Social Science Research: Theory and Principles .*Nairobi: Applied*.

Nerey H.M.M. (2012). Information System Security Effectiveness Attributes: A Tanzanian Company Case Study. *World Academy of Science, Engineering and Technology*(70), 551-557.

Nyawanga, J. O. (2015). *Meeting the challenge of cyber threats in emerging electronic transaction technologies in in Kenyan banking sector* (Doctoral dissertation, University of Nairobi).

Olayemi, O. J. (2014). A socio-Technological Analysis of Cybercrime and Cyber Security in Nigeria,*International Journal of Sociology and Anthropology*, 6(3), 116-125.

Osang, F. B., Ngole, J. &. Tsuma C (2013). Prospects and Challenges of M-learning Implementation In Nigeria: Case Study National Open University Of Nigeria (NOUN). International Conference on ICT for Africa.

Rajkumar, R. R., Lee, I., Sha, L., & Stankovic, J. (2010, June). Cyber-physical systems: the next computing revolution. In *Proceedings of the 47th Design Automation Conference* (pp. 731-736). ACM.

Ruighaver, A. B., Maynard, S., B. & Chang, S. (2007). Organizational Security Culture: Extending the End-User Perspective. *Computers & Security*, 26 (1), 56-62.

Santos, T. P. (2010). A Security Audit Framework to Manage Information System Security. *ICGS*(3), 9-18.

Serianu Consultants in Cyber Security (2015); available at ahttp://www.usiu.ac.ke/on-campus/news/296-serianu-usiu-africa-pkf-consulting-launch-kenya-cyber-security-report-2015

Sharma, R. (2012). Study of Latest Emerging Trends on Cyber Security and its Challenges to Society, *International Journal of Scientific & Engineering Research*, 3(6), 124-132

Sihanya, B. (2011). Confronting cyber crime in Kenya.

Siponen, Pahnila, and Mahmood(2010). Compliance with Information Security Policies: An Empirical Investigation.*Computer* 43(2), 64-71.

Slovic, P., Fischhoff, B., & Lichtenstein, S. (1977). Behavioral Decision Theory. *Annual Review of Psychology*, *28*(1), 1-39.

Solms R. and Solms B. (2004). "From policies to culture," *Computers & Security*, vol. 23, no. 4, pp. 275-279, 2004.

Straub, D. (1990). "Effective IS Security," *Information Systems Research*, vol. 1, no. 3, pp. 255-273.

Straub, D. (1990). Coping with Systems Risk: Security Planning Models for Management Decision Making. *MIS Quarterly* 22(8), 441-465.

Tarimo, C. (2006): ICT Security Readiness Checklist for Developing countries: A Social-Technical Approach. Ph.D thesis. Stockholm University, Royal Institute of Technology.

Tonge, A. M., Kasture, S. S., and Chaudhari, S. R. (2013). Cyber Security: Challenges for Society- Literature Review, *Journal of Computer Engineering*, 12(2), 67-75

Wechuli A. (2014) on Cyber Security Assessment Framework: Case of government Ministries in Kenya; *International Journal of Technology in Computer Science and Engineering*, 1(3).

Wekundah, R. N. (2015). *The effects of cyber-crime on e-commerce; a model for SMEs in Kenya* (Doctoral dissertation, University of Nairobi).

Zanoon, N., Albdour, N., & Hamatta, H. S. (2015) Security challenges as a factor affecting the security of manet: attacks, and security solutions. International Journal of Network Security & Its Applications (IJNSA) Vol.7, No.3, May 2015

Zhu, K., Kraemer, K. L., &Xu, S. (2002). A Cross-Country Study of Electronic Business Adoption Using the Technology-Organization-Environment Framework.

APPENDIX I: QUESTIONNAIRE

The purpose of this questionnaire is to obtained data which will be based on in carrying out a study seeking to find out factors affecting cyber security in the National Government Ministries in Kenya

Instructions for Part A: (Please complete appropriately by filling/ ticking in the sections provided)

SECTION A: GENERAL INFORMATION

1. Name of Ministry: _____

2. Which cluster of public service does your Ministry belong?

Security ( ) Public Administration & Social Services ( ) Infrastructure ( )

Education and Health ( ) Productive Sector ( )

3. Gender: Male ( ) Female ( )

4. Highest level of education: Diploma ( ) College ( ) University ( ) Masters ( )

5. Management Level: Audit management ( ) Audit staff ( )

ICT Management ( ) ICT Staff ( )

6. Work experience: Up to 5yrs ( ) 5 – 10years ( ) 10 – 15yrs ( )

15–20 yrs ( ) Over 20 yrs ( )

7. The Ministry use information systems in course of service delivery Yes ( ) No ( ).

8. Has the Ministry been a victim of cyber attack

Yes ( ) No ( ) Not sure ( )

9. Previous cyber attacks were targeted to?

Core functions ( ) Support Functions ( ) both core & support ( ) none ( )

10. What is the type of organizational structure does the Ministry's overall management apply? Centralized ( ) Decentralized ( ) Matrix ( )

11. What is the type of organizational structure does the Information System Administrators apply? Centralized ( ) Decentralized ( ) Matrix ( )

SECTION B: KEY MOTIVATION / DRIVERS OF CYBER-ATTACKS

1. Below are key drivers for cyber attacks in organizations. To what extent would you agree to each of the following drivers for cyber attacks in your Ministry?

   Use a scale of 1-5 where, 1= no extent, 2= little extent, 3= moderate extent, 4= large extent, and 5= very large extent.

Key Driver	**1**	**2**	**3**	**4**	**5**
Hacking exploitation (people trying out their hacking skills for challenge and peer status)					
Former Public Service employees disgruntled by their dismissal					
Serious and organized crime for financial gain					
Serious and organized crime for patent property theft					
Serious and organized crime for industrial knowledge or intellectual property theft					
Organized crime aiming at Ministry's systems / services sabotage					

Systems attack due to ideological and political extremism / differences					
Inter-states (other States governments' initiatives) cyber aggression					

SECTION C: FACTORS THAT MAY CONTRIBUTE TO CYBER SECURITY VULNERABILITIES

1. Below are several factors that may contribute to cyber security vulnerability in organizations. To what extent have these factors played a role of cyber security vulnerabilities at the Ministry? *Use a scale of 1-5 where, 1= no extent, 2= little, 3= moderate, 4= large, and 5= very large.*

Key Driver	**1**	**2**	**3**	**4**	**5**
Employees action derived for personal financial gains					
Disgruntled employees launching retaliatory attacks to sabotage systems / services delivery					
Unintentional employees actions but leading to systems attack					
Ministry cyber security policy and standards deficiency					
Poor implementation and adherence of cyber security strategy and standards by involved management					
Weak information infrastructure systems e.g. un-update systems patches					

Lack of clear identification and classification of ICT assets and exposure involved					
Employees non adherence to cyber security strategy & standards					
Employees poor cyber security awareness relative to ICT infrastructures, assets and exposures involved					
Poor cyber security responsiveness in line with cyber threats / attacks due to overall organizational structure					
Poor cyber security responsiveness in line with cyber threats / attacks due to IS organizational structure					
Ministry's management not acting as key leader in implementation and adherence of cyber security strategy and standards					
Ministry's management lack of provision of funds / support for sustainable cyber security systems					
Ministry's management lack of support for acquisition and development of Cyber security human skills (personnel)					
Lack of audit (review) of the Ministry cyber security capacity and adherence					
Management understanding of implications of cyber attacks to the Ministry's IS affects cyber security implementation					
Lack of legislative penalties for cyber attacks implication e.g. privacy details exposure					

Lack of market / environment pressure to sustain a high level of cyber security					