INFORMATION SECURITY THREATS AND E-GOVERNMENT INITIATIVES AT THE KENYA REVENUE AUTHORITY (KRA)

BY

GRAHAM MASINDE LUKORITO

D61/72867/09

A Management Research Project Submitted in Partial fulfilment of the requirements for the award of a degree of Master of Business Administration, School of business, University of Nairobi

November, 2012

DECLARATION AND RECOMMENDATION

Declaration

This Research is my original work and has not, wholly or in part, been presented for an award of a degree in any other university.

Graham Masinde Lukorito (D61/72867/09)

Signed: _____ Date: _____

Recommendation

This Research is the candidate's original work and has been prepared with my guidance and assistance; it is submitted with my approval.

Dr Kate Litondo

Supervisor

Signed: _____ Date: _____

Lecturer, Department of Management Science

School of Business

University of Nairobi

ACKNOWLEDGMENTS

My heartfelt sincere gratitude is to the almighty God for giving me good health and a sound mind to handle this project to its conclusion.

I am also very grateful to my supervisor Dr Kate Litondo for dedicating her valuable time and energy to ensure that I remained focused to finish the project. This project would not have been possible without her constant commitment and guidance to ensure that we achieve the best out of it.

I also would like to thank my wonderful parents Mr Benard Lukorito and Mrs Scrita Lukorito and my two loving sisters Sandra and Magda for their invaluable support, prayers and love. They provided consistent encouragement without which I would not complete this project

Last but not least I thank my friends, fellow MBA students, workmates, other lecturers and everybody else who in one way or another contributed ideas towards the improvement of this project. Their outstanding advise has seen me reach this far. Thank you all.

DEDICATION

I dedicate this project to my loving family for their consistent support and prayers. I thank God for they were truly a blessing to me. May the blessing of God be upon them.

ABSTRACT

Governments all over the world are embracing ICT to provide better services to the public. This use of information Technology has transformed the traditional form of government to E-Government. The Kenya government has invested a huge chunk of its budget on ICT although it is faced with complex and difficult questions regarding information security. The KRA being a major authority in the Ministry of Finance in the Kenyan government has also not being left behind in utilizing modern means of communication. KRA has also encountered several information security threats. Therefore the goal of this study is to determine the information security threats and e-government initiatives in the KRA.

The study had three main objectives. First it was to establish the security threats on e-government initiatives in the KRA. Secondly it was to establish the factors that facilitate security threats to e-government initiatives in KRA. Thirdly it was to determine the influence of security threats on e-government initiatives in the KRA. The study used case study design. This design was chosen since it is suitable for studies that concentrate on one key subject area like in our case the KRA. A direct contact questionnaire was used and we had 37 successful respondents out of a sample size of 40. The data analysis for the questionnaires used SPSS.

The study found out that software bugs, spamming and identity theft are the most common threats at KRA. These threats are facilitated by inadequate training, years an employee has worked at KRA, out dated software and social media. ITMS and Simba system are the most used system and are also prone to many of the threats. The information from this research will inform policy makers, government IT departments and other interested actors in the field of IT and internet security on the way forward in terms of policy formulation and implementation towards security and sustainable E-Governance in Kenya.

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

BOT –Build Operate and Transfer

CDs – Compact Disks

DDoS – Distributed denial of service attack

E-mail – Electronic Mail

ETR – Electronic Tax Number

GPRS – General Packet Radio Service

ICT- Information and Communication Technology

IPRs – Intellectual Property rights

I.T –Information Technology

KRA –Kenya Revenue Authority

PCs- Personal Computers

PIN – Personal identification Number

SPSS -Statistical Package for the Social Sciences

VAT – Value Added Tax

CHAPTER ONE: INTRODUCTION

1.1 Background of the Study

Governments all over the world want to improve their service delivery by satisfying the highest service priorities of people, businesses, communities, and employees by focusing resources to priority services (Smith & Jamieson, 2006). Information and Communication Technology (ICT) has transformed how the government provides these services to its citizens (G2C), businesses (G2B) , employees (G2E), governments (G2G) and religious movements (G2R) (Nikkhahan, Aghdam, & Sohrabi, 2009). The interaction between these diverse groups results in sharing and learning of new standards and technologies. This synergy yields better governance through proper utilization of ICT by making the government a one stop shop in taking care of its people at all levels in the society (Lyambila, 2010).

Investments in IT have offered governments the opportunity to deliver greater returns in revenue than almost any other conventional investment (Ataya et al., 2006). Governments are using the Internet to deliver services, disseminate information, and facilitate a more open dialogue between citizens and government (Schwester, 2009). Innovation and research in ICT has brought in new and evolving standards, tools and technologies that the government has been adopting, However, ICT provides an equally significant opportunity to destroy value (Ataya et al., 2006). Lately governments have been aggressively utilising various ICT tools and applications in rendering their services to the public such as the internet, mobile devices and wireless networks to enhance their services (Kessler, Hettich, Parsons, Richardson, & Triana, 2011).

1.1.1 Information Security

The general public views information security as recording, administering, and monitoring the actions and policies of government agencies (Smith et al., 2006). Information security is the protection of information systems against unauthorized access to or modification of information whether in storage, process, transit, and against denial

of service to authorized users, including those measures necessary to detect, document, and counter such threats (Andrews, 1999). Privacy can be defined as the absence of unreasonable, and potentially intrusive, collection and use of personal information. Therefore privacy is more of social factor while security is technical (Langenderfer & Miyazaki, 2009). The objective of information security is to preserve an organization's information assets and the business processes they support (Bell & Greg, 2001). Effective management of information risks and exposures can directly affect the profitability and overall value of an enterprise (Oliver et al., 2009).

Information security is more often done in reactive mode. A case in point is when the Kenya Police website was defaced in the year 2011, this made the security arm of the government to employ their public relations skills by hurriedly calling for press conferences to try to clear their name and correct public opinion after the incident (Madowo, 2011). The administration, business, and legal processes associated with security and protection of electronic government information have not been fully developed (Scott, 2003). Governments are beefing up their disaster preparedness through development of policies and procedures to improve security (Frank, 2003). Information security breaches are very dynamic in that they are constantly changing and becoming increasingly complicated to detect. Based on data collected from a broad cross-section of government organizations, the key information security implementation issues include awareness, active management support, training, and appropriate funding (Smith et al., 2006). When information security is put in proper use the cost benefit analysis outweighs the initials investment but the result of implementing wrongly is significant, including catastrophic financial losses and competitive disadvantage (Ataya et al., 2006).

1.1.2 Information Security Threats

An information security threat is any circumstance or event with the potential to harm an information system through unauthorized access, destruction, disclosure, and modification of data and/or denial of service (Yang, 2008). Hacking is a common threat and is the unauthorised access to a computer system by circumventing its security system (Chandler, 1996). Another threat is denial of service attack (DOS) whereby the attacker

floods the server or network with unnecessary commands, causing its resources to be consumed to the point where the service is no longer responding (Alfawaz, May, & Mohanak, 2008). Spamming is another threat. Spamming is the act of sending unsolicited bulk messages to many users at a time, possibly up to thousands, with the usual intention of advertising products to potential customers (Chandler, 1996).

Malware attack is another threat. Malware utilizes popular communication tools to spread, including worms sent through e-mail and messages, Trojan horses downloaded from websites, and virus-infected files downloaded from peer-to-peer connections they may also result from removable media including compact disks, thumb drives and mobile devices that are connected to computers (Yang, 2008). Software bugs also are a source of threats. It is an error, flaw, mistake, failure, or fault in a computer program or system that produces an incorrect or unexpected result, or causes it to behave in unintended ways (Yang, 2008). Over privileged users are also sources of a threat. Users should be given permission that is just enough to perform their duties (Chandler, 1996).

There are many factors that cause these security threats. One of them is hiring young employees. Hiring young employees can bring in fresh talent and innovation in an organization, However they are also a source of information security risk. 70 percent of generation Y (younger employees) frequently ignore laid down information security policies. If this age group is accustomed to sharing complete details about their personal lives on social media sites like “facebook” and “twitter”, how can they be entrusted with company sensitive data (Cisco Connected World Technology Report, 2011). Computer literacy is also another factor. Computer studies are part of today’s school curriculum and a key requirement to finding employment. Therefore employees can use their computer knowledge to find loopholes and faults in information systems (Gauci, 2008). Lack of awareness is another factor. End users of the system need to be informed of why it is important to follow security guidelines. These users will likely share passwords, share flash disks and compact disks and open emails without scanning. They will also browse websites that contain suspicious links; hence such actions may compromise the government security system and expose them to various security threats. The end-users may not be aware of security challenges; they may hold certain attitude, assumptions and

values towards the use of information security policies put into place (Alfawaz, May, & Mohanak, 2008).

The usage of various ICT tools and modern applications by the government has increased the level of insecurity of Information systems (Kessler, Hettich, Parsons, Richardson, & Triana, 2011). Such security threats affect government operations in various levels. The government needs to ensure that information and information processing systems are available when information is required (Evans, 2003). These threats can lead to denial of service, compromise of data integrity, loss of critical information, wasted time in restoring information from backups and huge costs incurred on hiring human labor to be in charge of information security and costs of purchasing firewalls and security software (Alsmadi, 2011). Some threats also lead to increased fraud and the government name being tarnished (Mbuvi, 2012). When citizens feel that the government website is prone to attacks, they may discourage the government from adopting ICT (Stibbe, 2005).

1.1.3 E-Government

E-Government is whereby government agencies use information technologies such as Wide Area Networks (WAN), the Internet, and mobile computing that have the ability to transform relations with citizens, businesses, and other arms of government. These technologies can serve a variety of different ends such as better delivery of government services to citizens, improved interactions with business and industry, citizen empowerment through access to information, or more efficient government management. The resulting benefits can be less corruption, increased transparency, greater convenience, revenue growth, and/or cost reductions (The World Bank Group, 2011). It can also be defined as the important transformation of public sector internal and external relationships through net-enabled operations, information technology and communications (ICT) to optimize government service delivery, citizen participation and governance (Gartner Group, 2012). E-government is analogous to e-commerce, which allows businesses to transact with each other more efficiently (B2B) and brings customers closer to businesses (B2C), e-government aims to make the interaction between government and citizens (G2C), government and business enterprises (G2B),

and inter-agency relationships (G2G) more friendly, convenient, transparent, and inexpensive (The World Bank Group, 2011).

E-Government is viewed differently by members of the society. Some feel it is a simple website where political and government issues are regularly posted, but this outlook demeans the range of opportunities it offers (Ndou, 2004). E-Government is not limited to administrative uses but encompasses e-citizens, e-services and e-society (Fallahi, 2007). Most people refer to e-government as digital/connected/online government. Traditionally, the interaction between a citizen or business and a government agency took place in a government office. With emerging information and communication technologies it is possible to locate service centers closer to the clients. Such centers may consist of an unattended kiosk in the government agency, a service kiosk located close to the client, or the use of a personal computer in the home or office (Bhattacharya & Goswami, 2011).

The fundamental owners of e-government are the politicians. Politicians accountability, commitment, engagement and active ownership are vital drivers for e-government progress, public investment in core Government efforts, policy making and public sector reform is essential for service delivery (Kessler, Hettich, Parsons, Richardson, & Triana, 2011). The government is expected to behave like a firm in that it has to constantly adopt new methods to improve its operations with time. Ansoff (1998) stated that a firm that does not improve its performance sooner or later will lose its competitive advantage and eventually drop out of the market. The government expects to get value for money from the public purse by ensuring its agencies operate within their budgets, rigorously pursue efficiencies, streamline regulatory systems, and cut "red tape" (Smith et al., 2006). The following are the six major categories affecting the quality of an e-government website: Security and privacy, usability, content, services, citizen participation and feature (Henriksson et al., 2006). From the list mentioned concentration was on information security and privacy and how it affected e-government initiatives.

1.1.4 E-Government in Kenya Revenue Authority (KRA)

E-Government was transferred to African countries as a solution to corrupt governance by carriers such as international donor agencies, consultants, Information Technology vendors and Western-trained civil servants (Ochara, 2008). The Kenya Revenue Authority (KRA) was established by an Act of Parliament, Chapter 469 of the laws of Kenya, which became effective on 1st July 1995. The Authority is charged with the responsibility of collecting revenue on behalf of the Government of Kenya. KRA has the following major systems that support e-government: Simba system, ITMS and ETR (KRA, 2011).

Simba system is an online based system that provides for a single point of entry declarations. It was introduced in the year 2005 as a replacement of the Orbus system. It has automated the various tasks of custom clearance from custom declaration to payment of dues. It is used by shipping, clearing agents and KRA officers. This customs clearance system was meant to speed up clearance of cargo as well as eradicate corruption at the port. So far it has reduced a backlog of consignments by clearing an average of 1,700 containers per day. It is a web based system running on an oracle database backend (KRA, 2011). Simba system employees have been accused of sabotaging the system which leads to reverting to the manual system. During the downtime, tax evasion cartels pass in contraband goods as well as evade taxes (Marete, 2011). The ITMS (Integrated Tax Management System) is an online system that makes it easy for tax payers to file returns. The system is used by tax payers, agents, and KRA officers. The system is used for tax payer registration for both individuals and companies. It can be used to generate the PIN (Personal Identification Number) certificate. The system can also be used to verify someone else PIN number (KRA, 2011).

Electronic Tax Registers (ETR) is a machine that is to be used by traders who supply taxable goods and services. The ETR machine is used to automatically account for sales. It has a fiscal memory and a special read only memory to store tax information at the time of sale. KRA introduced it to create a level playing field for all traders and improve revenue collection to benefit all Kenyans. Since its introduction, the ETR has made it harder for unscrupulous traders from cheating on their Value Added Tax (VAT) hence

increasing the government's revenue. KRA is currently planning to upgrade the ETR with a new device that is General Packet Radio Service (GPRS) enabled. GPRS makes it easier to monitor tax payers. The new device can be located remotely and this reduces the risk of losing data because the device is stolen. The new devices will relay information back to KRA servers (KRA, 2011).

1.2 Statement of the Problem

Prior to e-government, records were stored on paper which required a lot of manual effort to copy. Tampering the paper was hard as one needed to also forge the paper colour, type, size and texture. Those security measures focused on the physical protection of the document and restricting physical access to the records (Smith et al., 2006). Electronic documents unlike paper can be downloaded and copied in nanoseconds (Backhouse & Dhillon, 2001). The government being the single largest collector of citizen data has over time amassed a great deal of state secrets concerning its citizens, employees, financial and its security systems (Kessler et al., 2011). The rapid growth in volume of electronic data stored by the government increases the need for security systems to protect the privacy of this information and prevent fraud (Smith et al., 2006). Security is traditionally concerned with information properties of confidentiality, integrity and availability (Alfawaz, May, & Mohanak, 2008).

When information lands in the wrong hands, it can lead to expensive law suits, civil strife, terrorism, wars, political instability that can eventually culminate to the government being overthrown, Hence the need to protect the sovereignty and territorial integrity of a country (Kanhere, 2009). The concept of Information Security as it affected the Kenya governments as a major concern was brought to the limelight after the infamous "wikileaks" scandal. "Wikileaks" is a website that notoriously publishes leaked highly sensitive documents from government cables including the government of Kenya (Assange, 2006). It emerged that as the Kenya government continued to adopt high tech communication methods, they innocently became vulnerable to information security breaches and attacks both from within and without. While rapid growth of information

and communication technology in government can facilitate improved service provision, it can also pose a privacy threat (Kessler, Hettich, Parsons, Richardson, & Triana, 2011).

Previous related studies done are like the "Emergence of the E-Government Artefact in an Environment of Social Exclusion in Kenya" and "Managing the E-Government Adoption Process in Kenya's Local Authorities" by Nickson Muganda both in the year 2008 focused on e-government itself, however this study will go as step further to look at the effects of security threats directly and indirectly affecting the initiatives of e-governance in the Kenya Revenue Authority. According to (Alfawaz, May, & Mohanak, 2008), security threats lead to denial of service attack. Therefore, this study answered the following questions: What were the security threats? What factors facilitated the security threats? What influence did the security threats have on e-government initiatives at the KRA?

1.3 Objectives of the Study

The general objectives was to establish the effect of security threats on e-government initiatives in the KRA specifically

a. To establish security threats on e-government initiatives in the KRA
b. To establish the factors that facilitate security threats to e-government initiative in KRA
c. To determine the influence of security threats on e-government initiatives in the KRA

1.4 Value of the Study

There has been a major focus on information security challenges in the commercial sector especially banking. The government had been neglected due to its earlier sluggish pace in adopting IT which was hampered by its bureaucracy. The government of Kenya plans to achieve vision 2030 by embracing ICT in its various operations such as elections, education, tax filing, and procurement among others. This study will guide the government especially KRA on the security challenges that they should be aware of that come as a result of adoption of the rapidly evolving complex information systems. Generally few countries in Africa have the appropriate legal and regulatory framework

that have the capacity to handle ICT security challenges. The study established the security threats that affect the government which will help the government come up with better policies. Since the security challenges cut across many industries as well this study will build on knowledge that can also be used by banks, insurance and many more organisations in protecting their information assets

CHAPTER TWO: LITERATURE REVIEW

2.1 Introduction

In this chapter, literature relevant to the topic of information security threats and e-government initiatives in the Kenya Revenue Authority (KRA) was reviewed. The chapter highlighted the concept of e-government, security and threats to information and its effects on the e-government initiatives in KRA.

2.2 Information Security

Information security threats that affect E-Commerce are very similar to those affecting e-government (Nikkhahan, Aghdam, & Sohrabi, 2009). The difference lies in that the government is mandated to serve the whole country but the business deals with a subset that it wishes to. The government networks communicate with each other better than business networks because businesses do not want to disclose sensitive information to their competitors (Stibbe, 2005). The business has full control of its own network but the government needs to liaise with many heterogeneous systems. The government in its possession keeps very sensitive information about itself, its citizens thus security for the government is more crucial than the business unit (Conklin & White, 2006). Unlike typical websites that include largely data to browse and download, e-government portals are expected to have sensitive private personal data about country citizens.

The threat of possible intrusion or identity theft is high and may cause serious consequences (Alsmadi, 2011). With the increasing dependence of the corporate world and governments on information systems and technology, the need, importance and relevance of information security governance is well acknowledged and accepted by top management. The questions that still plague organizations at all levels are not whether, why or what to secure; the business policies and risk management framework provide the answers to these questions. Questions of when, how, to what extent and at what cost to secure business and its information systems remain (Kanhere, 2009). The increasing threats and vulnerabilities in a networked and connected world, the growing use of information technology in almost all fields, and the high value of information in today's environment have resulted in a demand for information security standards and their

effective implementation to protect information assets (Humphreys, 2009). The efficiency of electronic data management facilitates integrated citizen information, but also introduces complex requirements for controls and processes (Kessler et al., 2011). The widespread adoption of ICT creates common fears such as intrusive data collection, misuse of personal information and constant surveillance (Kessler, Hettich, Parsons, Richardson, & Triana, 2011).

2.3 Information Security Threats

A threat is any circumstance or event with the potential to harm an information system through unauthorized access, destruction, disclosure, and modification of data and/or denial of service (Yang, 2008). One threat is cyber-crime which is a criminal activity done using computers and the Internet. Examples include creating and distributing viruses on other computers or posting confidential business information on the Internet (Yang, 2008). The most prominent form of cybercrime is identity theft, in which criminals use the Internet to steal personal information from other users. They can then impersonate the other users and compromise security (Yang, 2008). Hacking is a threat whereby one gains unauthorised access to a computer system (Chandler, 1996). Some hackers do so for fun, search for crucial data while others want to fulfil their polical objectives (Yang, 2008). The other threat is theft of information in electronic form. This theft is either physically removing hard disks or tampering with them virtually. Networking has facilated virtual theft (Chandler, 1996).

Email bombing and spamming is a kind of activity that refers to sending large numbers of mail to the victim, who may be an individual, company or mail servers thereby ultimately resulting into crashing their servers. Spamming is the act of sending unsolicited bulk messages to many users at a time, possibly up to thousands, with the usual intention of advertising products to potential customers. Spamming can also be used as a form of irritation by singling out an email address and sending the owner of that address hundreds of emails per second (Chandler, 1996). Spamming is usually random and untargeted but it can be targeted to either a group of people, for example, advertisements that cater for a particular group of people, or certain persons, like in the case of spamming for the purpose of irritating the public (Smith & Jamieson, 2006). In Kenya Serianu Cyber

Intelligence Team (SCIT) found 150 spam sending IP addresses that are owned by Internet Service Providers (ISPs) located in Kenya between January and April 2012 (Makatiani, 2012).

Software bug are also threats. The bugs arise from mistakes and errors made by programmers in a program's source code, design, or by compilers producing incorrect code. They usually arise if a computer system was not properly tested or there was no proper change management, therefore bugs can expose security flaws where users can bypass access controls to obtain unauthorized privileges (Yang, 2008). Data diddling is the kind of a threat that involves altering raw data just before a computer processes it and then changing it back after the processing is completed. In India the electricity board faced similar problem of data diddling while the department was being computerised (Grabosky, Smith, & Dempsey, 2001). A salami attack is the kind of threat normally prevalent in the financial institutions for the purpose of committing financial crimes. An important feature of this type of offence is that the alteration is so small that it would normally go unnoticed. An example is the Ziegler case wherein a logic bomb was introduced in the bank's system, which deducted 10 cents from every account and deposited it in a particular account (Grabosky, Smith, & Dempsey, 2001). Denial of Service attack is where the computer of the victim is flooded with more requests than it can handle which causes it to crash. Distributed Denial of Service (DDoS) attack is also a type of denial of service attack, in which the offenders are wide in number and widespread (Alsmadi, 2011).

Viruses are programs that attach themselves to a computer or a file and then circulate themselves to other files and to other computers on a network. They usually affect the data on a computer, either by altering or deleting it. Worms, unlike viruses do not need the host to attach themselves to. They merely make functional copies of themselves and do this repeatedly till they eat up all the available space on a computer's memory. The world's most famous worm was the Internet worm let loose on the Internet by Robert Morris in 1988 which almost brought development of Internet to a complete halt (Coleman, 2002). Logic bombs are event dependent programs. This implies that these

programs are created to do something only when a certain event/trigger occurs. Some viruses may be termed logic bombs because they lie dormant all through the year and become active only on a particular date like the Chernobyl virus (Yang, 2008). Trojan attacks originate from the word 'Trojan horse'. In software field this means an unauthorized programme, which passively gains control over another's system by representing itself as an authorised programme. The most common form of installing a Trojan is through e-mail. Web jacking attack is derived from the term hi jacking. In these kinds of offences the hacker gains access and control over the web site of another. He may even mutilate or change the information on the site. This may be done for fulfilling political objectives or for money. In the year 2006 the site of MIT (Ministry of Information Technology) of India was hacked by Pakistani hackers and some obscene matter was placed therein (Yar, 2006).

Intellectual Property crimes (IPR*)* is any unlawful act in which the owner is deprived completely or partially of his rights. The common form of IPR violation may be said to be software piracy, copyright infringement, trademark and service mark violation, theft of computer source code. Piracy involves the illegal reproduction and distribution of software applications, games, movies and audio CDs (Longe, 2004). Pirates usually buy one original version of a software, movie or game and illegally make copies of the software available online for others to download and use without the notification of the original owner of the software. This is known as Internet piracy or warez. The term "warez" describes commercial software, movies and games that has been modified by a cracker and made freely available to the public on the Internet (Longe, 2004). In Africa there has been a small increase in the piracy rate, from 52 percent in 2000 to 53 percent in 2001. South Africa, the largest economy in the region, had the lowest piracy rate, at 38 percent. Kenya has 77 percent and Nigeria 71 percent which were the two countries in the region with the highest piracy rate. Kenya recorded the highest number in pirated software and operating system (Sembok, 2003).

2.4 Factors that Facilitate E-Government Security Threats

There are various factors that facilitate security threats to the government information systems. Computer literacy is a common prerequisite to be offered either formal or informal employment. It is one of the fundamental skills required by those in employment and those returning back to work (Gauci, 2008). “Direxer” the alleged hacker of 103 Kenyan government websites alleged that he used tutorials of an Indonesian forum known as Forum Code to hack the websites (Mbuvi, 2012). The more I.T knowledge people are the more the chances of them identifying loopholes in the system. The age of an employee is also another factor. Younger employees are well versed with IT skills but are likely to ignore laid down IT security policies. 70 percent of the young employee may probably use identity theft or steal access rights to access sensitive data they are not supposed to. The young employees are also used to sharing data on social networks and will likely share secretive government data when employed (Cisco Connected World Technology Report, 2011).

Social media includes web and mobile-based technologies which are used to turn communication into interactive dialogue among organizations, communities, and individuals (Kaplan & Michael, 2010). Before social media, the distribution of both personal and corporate information was hard and complicated however Social media has provided the opportunity for anyone to post information that would be seen by all and sundry. The same way social media can be used by the marketing and public relations (PR) deparment to advertise their product is the same way sensitive government data can easily be leaked to the public through social media (Bahadur, 2012).

Technology and innovation often catch on ahead of regulation. These innovations and levels of growth in information systems were not envisioned by the regulatory framework (Omwansa, 2009). Innovation and changes in information technology is quite dynamic as compared with legislation which is rigid and is supposed to regulate and govern it. There is a shortage of relevant laws and policies that govern information security (Hwang, Li, Shen, & Chu, 2004). Central bank of Kenya took a long time to come up with policies to govern mobile money transfer like M-pesa as compared to prudent regulation it has on

banks and other conventional licensed financial institutions. Although not tighetning regulation on information technology will encourage innovation, reduce costs of transactions and grow the economy, hackers can use new innovations maliciously before regulations are put into place (Omwansa, 2009).

Many government agencies do not regularly update their software and antivirus. This makes them very vulnerable as cyber criminals can easily take advantage of the loopholes and bugs in older software versions than when one is using a newer one. The government is not proactive in protecting its sites and until it is attacked that is when it will try to salvage itself (Makatiani, 2012). There is also plethora of computing devices like laptops, tables PCs and also mobile phones. Some of these devices are embedded with cameras referred to as webcams. Experienced hackers can access ones webcam in less than a minute and access sensitive information (Kash, 2012). Unsecured wireless networks (WIFI) and government websites that are not using secure socket layer (SSL) make it very easy for hackers to connect to their networks and steal passwords since that communication is not encrytped. Once the passwords are stolen they can be used to gain access to sensitive information (Abrams, 2010).

2.5 Influence of Security Threats on E-Government Initiatives

E-government security is considered one of the crucial factors for achieving an advanced stage of e-government (Alfawaz, May, & Mohanak, 2008). The impact of a successful attack on an organisation information asset will depend on how, and to what degree, the organisation's operations are disrupted. Hacking of government websites can lead to loss of data integrity. Hackers can tamper with critical information and replace with misleading data. If the governments lacks proper backup and restore policy, it will take a long time and resources to restore lost data (Alsmadi, 2011). Security threats such as spamming lead to denial of service for the citizens (Alfawaz, May, & Mohanak, 2008). This is done when an intruder floods the government website with many repetitive, long running requests that lead to shutting down the webservers. Such attacks leads to majority of the citizens being unable to access important information from the government domain (Alsmadi, 2011).

These security threats also have a cost implication. Spamming increases bandwidth charges for the government as a result of increased network traffic. The government will end up paying for wasted bandwidth to its ISP, and will also incur additional costs in restoring data and from the downtime. Spamming attacks also causes problems for the government and citizens because of increased fraud, wasted time, and various other scams. Much time and money will be wasted trying to recover lost data from the backups (Makatiani, 2012). These security threats also lead to the government name being tarnished. In the case of 103 Kenya government websites that were attacked in January 2012, this led to the public image of the government waning (Mbuvi, 2012). E-government role is to provide its services anywhere and anytime over the network. "Wikileaks" published a report describing the Kenya government as corrupt and described the weakness of the character of Kenya leaders. Such leakage of government cables led to Kenya reputation being spoilt all over the world (Assange, 2006). These threats lead to the citizens becoming afraid to have their data posted online and eventually lead to poor utilization of e-government websites. The citizen may prefer using manual systems which they are used to and trust (Stibbe, 2005).

2.6 E-Government

E-Government provides nonstop government information for the citizens, enterprises, government officers, public administrators and agencies over a network (Hwang, Li, Shen, & Chu, 2004). Governments of many countries across the globe, today at all levels respond to millions of citizen's demands electronically hence governments are fairly functional in the cyberspace through facilitating electronic transactions and delivery of services and information to businesses, citizens and governments agencies (Bhattacharya & Goswami, 2011). E-governance features include being open for business 24 hours a day, greater accessibility, lower costs and not having to visit government offices physically; it also aims to provide government information electronically (Gilmore & D'Souza, 2006). The increasing use of information and communications technologies (ICTs) by governments has primarily been encouraged by a trend where many governments have been reforming their public sector in order to meet the aspirations of their citizens (Ochara, 2008). E-government is simply not buying computers for majority

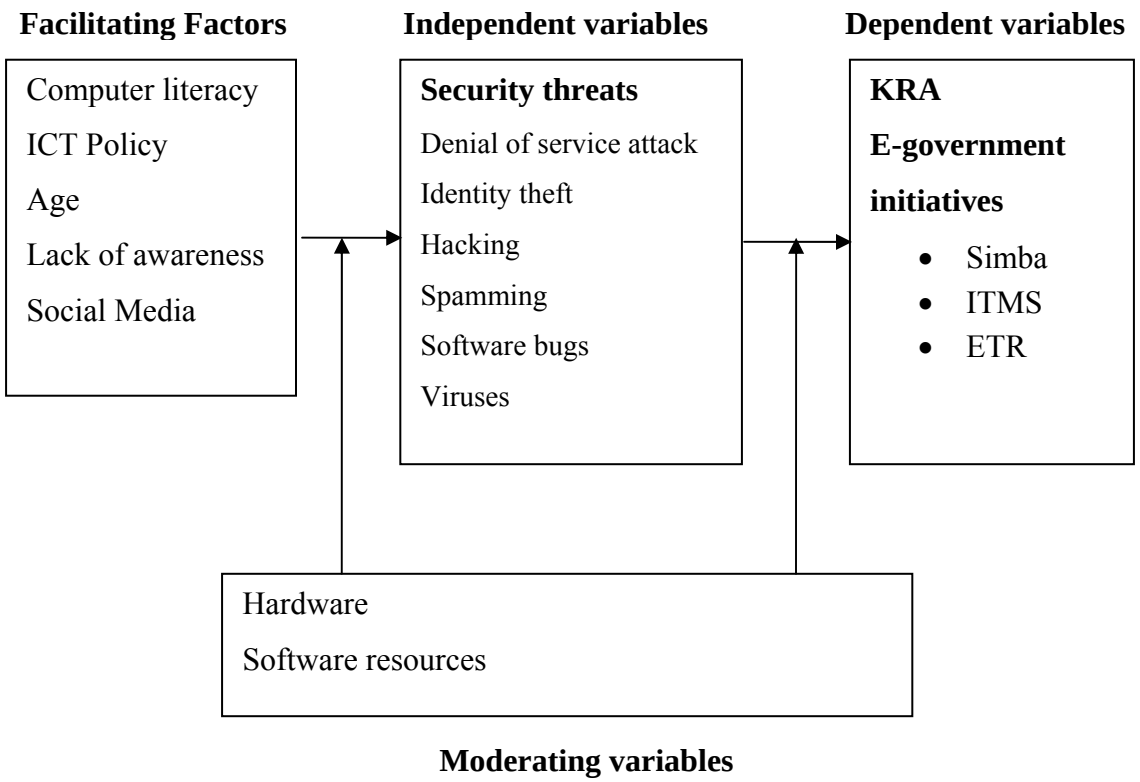
of government employees but encompass the broader picture of corporate governance. Corporate governance has various dimensions such as transparency, accountability, stakeholders' interest, ethics and fair play (Kanhere et al., 2009). E-government serves the various functional units of government including management, marketing, operations, logistics, finance, accounting, supply chain management and human resource management.

The government of Kenya is embracing cloud computing. Kenya telecoms operator Safaricom launched the biggest indigenous public cloud in Africa known as "SafaricomCloud" in October 2011 at a cost of over USD20 Million (Biztech Africa, 2011). Cloud computing is online-based computing in which shared resources such as network, software and information are provided to computers and other devices on demand thus clients essentially pay a single license to receive a host of services as opposed to paying for each individually (Safaricom, 2011). The government of Kenya will be the first client to adopt "SafaricomCloud" as its data services are running out of capacity. The cloud will break the physical barrier between the government systems and the citizens (Ransome, 2009). Even though the cloud continues to grow in popularity and respectability; complications with data privacy and data protection still plague the market (Hubbard, 2009).

2.7 Conceptual Framework

From the literature review, facilitating factors are the contributing factors that make it easier for security threats to take place. They are the prerequisites for information security threats in e-government initiatives which are the independent variables. Examples of the factors include computer literacy, ICT policy, social media, age and lack of awareness. Independent variables are the various security threats that affect e-government. These threats affect the dependant variables. Independent variables include threats such as identity theft, spam, hackers and viruses. Dependant variables are based on the KRA e-government initiatives that include Simba system, ITMS, and ETR. Control variable affect both the independent variables and dependant variables. Examples include personal characteristics, hardware and software resources. This study will investigate how the variables affect each other. Figure 1 below shows the relationship in a diagram

Figure 1: Conceptual Framework



Source: own compilation

CHAPTER THREE: METHODOLOGY

3.1 Introduction

This chapter focused on the methodology that was used in the study. It was organized under the following subheadings; research design, population size, sample size and sampling procedure, instrument of data collection, data analysis and presentation.

3.2 Research Design

This study used the case study design (Mugenda, 2008). Case study is conducted where there is an intensive analysis for an individual study context to capture all pertinent aspects. This method was selected as this study dwells heavily on the KRA. The typical statistics that are used in case studies are measures of dispersion and central tendency. Variance and standard deviation are the most common measures of dispersion while the mean, median and mode are the most common measures of central tendency.

3.3 Population, Sample Size and Sampling Procedure

The KRA Information Technology (IT) has around 170 employees. Therefore 170 will form our population. The sample was based on 40 employees of the KRA who are in Information Technology department who were selected through purposive sampling. Purposive sampling is used to reduce the occurrence of undesired and duplicate responses (Mugenda, 2008). The sample of 40 was composed of 6 employees from each of the following units: support, development, website, I.T audit and networking.

3.4 Instrument of Data Collection

A direct contact questionnaire was used as a primary tool for data collection in this study. The direct contact questionnaire was found suitable as it makes it possible to establish rapport with the respondents. It also leads to minimal wastage of time and loss of questionnaires (Borg & Gall, 1983). One set of questionnaires (Appendix I) was administered to the respondents in the KRA.

3.5 Data Analysis and Presentation

We used the two regression mode to analyse the data. The data analysis for the questionnaires made use of the SPSS software. Objective 1 was answered by section A of the questionnaire which used descriptive statistics for analysis where frequencies, percentages and mean was calculated and presented by charts and graphs. Objective 2 was answered by section B of the questionnaire which used the regression model as illustrated in Equation 1.

$Y= a_0 + a_1x_1 + a_2x_2 + a_3x_3 + e$ (Equation 1)

Definition

Y = Information security threats

X_1 = Determinants of security threat

X_2 = ICT Resources

X_3 = Personal Characteristics

e = Error term

Objective 3 was answered by Section C of the questionnaire which used the regression model as illustrated in Equation 2 below

$Y_1= a_0 + a_1x_1 + a_2x_2 + a_3x_3 + e$ (Equation 2)

Definition

Y_1 = KRA e-government initiatives

X_1 = Information security threats

X_2 = ICT Resources

X_3 = Personal Characteristics

e = Error term

CHAPTER FOUR: DATA ANALYSIS AND PRESENTATION

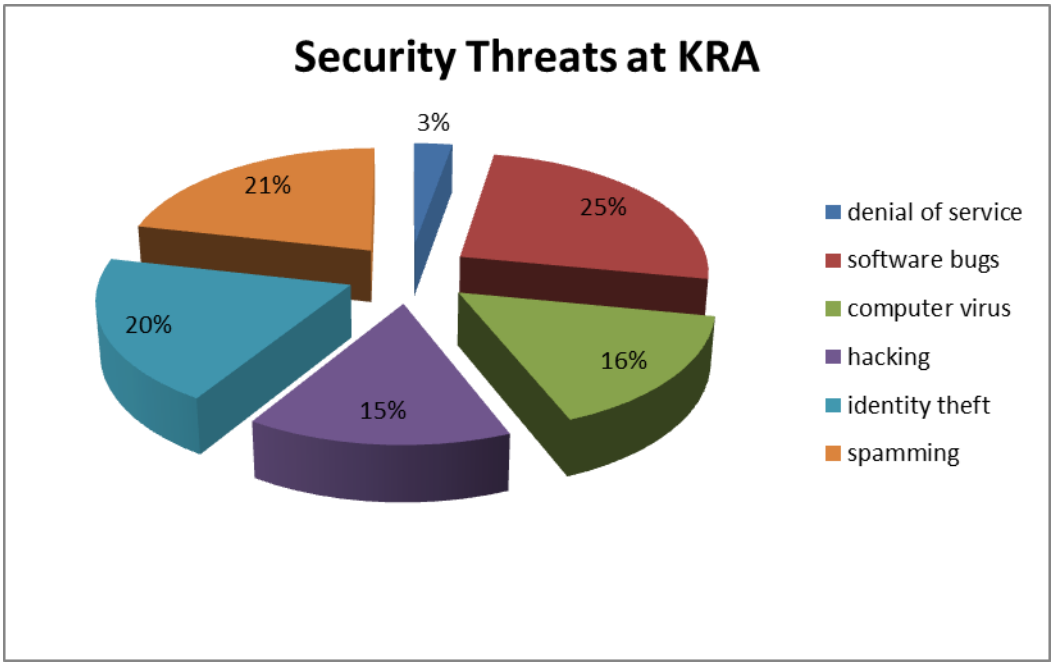
4.1 Introduction

This chapter presents the data analysis and interpretation of the research findings to address the study objectives. Data was collected from Kenya Revenue Authority (KRA) employees through a questionnaire. The total number of respondents who returned their questionnaires was 36 out of 40. This figure is 90% of the sample that was selected.

4.1.1 Security Threats at KRA

KRA faces various security threats in different proportions. Software bugs is the most common threat at 25% of all the threats followed by spamming at 21% and Identity theft at 20% as shown by Figure 2. Denial of service attack is the least threat at 3%. Computer virus is at 16% while hacking takes 15% of all the threats.

Figure 2: Security Threats

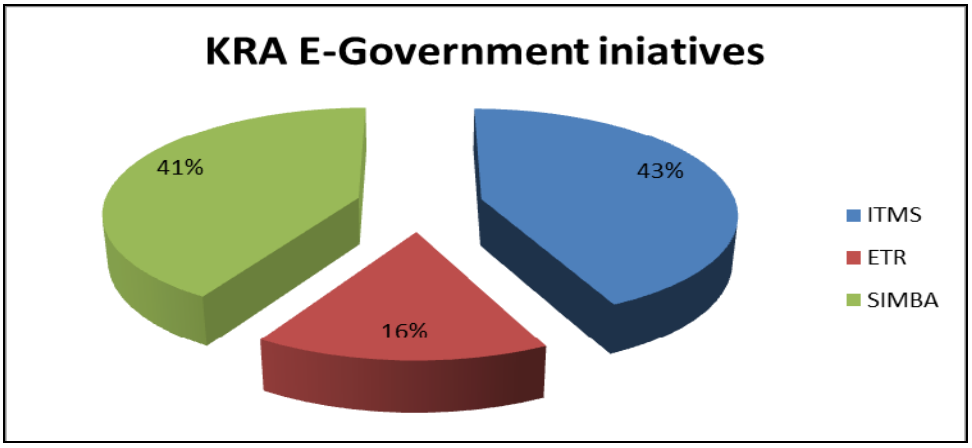


Source: Research Data

4.1.2 E-Government Initiatives

KRA e-government initiatives involve and are not limited to the following: Simba, ITMS and ETR. ITMS system is the most common used system by the respondents at 43% followed closely by SIMBA at 41% and ETR at 16% as shown in Figure 3 below.

Figure 3: E-Government initiatives in KRA

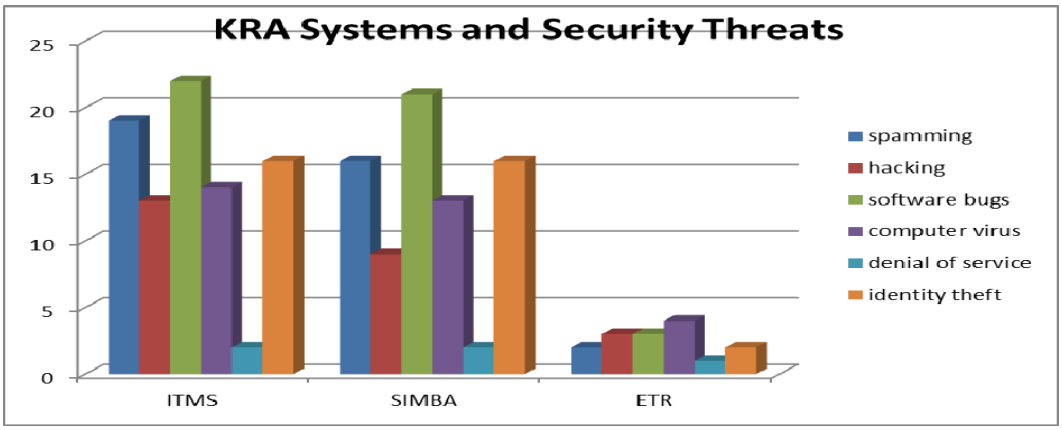


Source: Research Data

4.1.3 KRA Systems Security Threats

Simba and ITMS systems have more threats as compared to ETR as shown by Figure 4. This can be due to they are the most used systems as illustrated by Figure 3 above. Spamming, identity theft and software bugs threats affects all the KRA systems the most. Denial of service and hacking are the threats with the least effect on the KRA e-government initiatives. ETR has computer virus as its most severe threat.

Figure 4: KRA Systems and Security Threats



Source: Research Data

4.1.4 Factors that Facilitate Information Security Threats at KRA

These factors are the conditions that make it easier for information security threats to attack.

4.1.4.1 Age and Spamming Cross Tab

Majority of the respondents of the age bracket of 26 to 30 years experienced the most spamming threats at 9 out of 36 as shown by figure 5. This was followed closely by the age group of 31 to 35 years who were affected by spamming attack at 8 out of 36. Overall the young age group were more prone to spamming attack compared to the older age groups which had either 0 or 1 spam attack.

Figure 5: Age and Spamming Cross Tab

age bracket * spamming Crosstabulation

Count

		Spamming		
		Yes	No	Total
age bracket	25 or Younger	4	0	4
	26 to 30	9	1	10
	31 to 35	8	0	8
	36 to 40	1	5	6
	41 to 45	1	5	6
	46 or older	0	2	2
Total		23	13	36

Source: Research Data

4.1.4.2 Social Media Influence on Computer Virus

Employee access of social medial in the office correlates with computer virus at R=.622 by Figure 6a) which is a high degree of positive correlation. Adjusted R square = 36.9% which means usage of social media can explain 36.9% of computer virus. Since this model is P< 0.005 which is less than 0.05 according to Figure 6b) implies that the model is good enough to predict the outcome of the computer virus variable. The coefficient of correlation shows that for every unit increase of social media we expect a 62.5% increase of computer virus threat on Figure 8c)

Figure 6a): Model Summary of Social Media and Computer Virus

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.622[a]	.387	.369	.402

a. Predictors: (Constant), access social media

Figure 6b): Anova Model of Social Media and Computer Virus

ANOVA[b]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	3.472	1	3.472	21.465	.000[a]
	Residual	5.500	34	.162		
	Total	8.972	35			

a. Predictors: (Constant), access social media

b. Dependent Variable: computer virus

Figure 6c): Coefficient of Correlation Model of Social Media and Computer Virus

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	.625	.206		3.033	.005
	access social media	.625	.135	.622	4.633	.000

a. Dependent Variable: computer virus

Source: Research data

4.1.4.3 Years Worked at KRA with Spamming Threats

Years worked at KRA correlates with spamming threats at R= .766 which means there is a positive high degree of correlation between years at KRA and spamming as shown by figure 7a). The adjusted R square=57.4% which means spamming can be explained by

57.4% by years worked at KRA which is quite high. Figure 7b) shows P< 0.005 which is less than 0.05 which indicates that the model applied is significantly good enough to predict the outcome variable. The coefficient of the variables in Figure 7c) shows that an increase in a unit of years at KRA reduces spamming threats by 28.8% and P<0.005 which is less than 0.05 which indicates that the model is good enough to predict the outcome of the variable. Thus the more one works at KRA the less they will get spamming threats.

Figure 7a): Model Summary of Regression of Years Worked at KRA with Spamming

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.766[a]	.586	.574	.318

a. Predictors: (Constant), How many years have you been at KRA

Figure 7b): Anova model of Years Worked at KRA with Spamming

ANOVA[b]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	4.871	1	4.871	48.221	.000[a]
	Residual	3.435	34	.101		
	Total	8.306	35			

a. Predictors: (Constant), How many years have you been at KRA

b. Dependent Variable: spamming

Figure 7c): Coefficients Model of of Years Worked at KRA with Spamming

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	2.201	.132		16.670	.000
	Years worked at KRA	-.288	.041	-.766	-6.944	.000

a. Dependent Variable: spamming

Source: Research Data

4.1.4.4 Out dated Software Influence on Software Bugs Threats

Out dated software correlates with software bugs threats at R=.501 as shown by Figure 8a) which is a very high positive degree of correlation. Adjusted R squared = 22.9% which means out dated software can explain 22.9% of software bugs threats which is moderate. Since this model is P< 0.005 which is less than 0.05 according to Figure 8b) implies that the model is good enough to predict the outcome of the variable. For every unit of increase in out dated software there is 45.2% increase in software bugs as shown by figure 8c)

Figure 8a): Model Summary of out dated software on Software Bugs

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.501[a]	.251	.229	.386

a. Predictors: (Constant), have outdated software

Figure 8b): Anova Model of out dated software on Software bugs

ANOVA[b]

Model		Sum of Squares	Df	Mean Square	F	Sig.
1	Regression	1.693	1	1.693	11.384	.002[a]
	Residual	5.057	34	.149		
	Total	6.750	35			

a. Predictors: (Constant), have outdated software

b. Dependent Variable: software bugs

Figure 8c): Coefficients of Correlation Model of Out dated software and Software bugs

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	T	Sig.
		B	Std. Error	Beta		
1	(Constant)	.635	.193		3.290	.002
	have outdated software	.452	.134	.501	3.374	.002

a. Dependent Variable: software bugs

Source: Research data

4.1.4.5 Information Security Policy Awareness and Spamming

Employee knowledge of information security policy correlates with Spamming threats at R=.506 on Figure 9a) which is a high positive degree of correlation. Adjusted R squared = 23.4% which means employees knowledge of security policy can explain 23.4% of spamming threats which is moderate. Since this model is P< 0.005 which is less than 0.05 according to Figure 9b) implies that the model is good enough to predict the outcome of the variable. For each single unit of security policy awareness there is decrease of 52.7 in spamming as shown by Figure 9c). Hence employee knowledge of policy reduce spamming threats

Figure 9a): Model Summary of Employee Know Policy and Spamming

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.506[a]	.256	.234	.426

a. Predictors: (Constant), Do employees know IS policies

Figure 9b): Anova Model of Employee Know Policy and Spamming

ANOVA[b]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	2.124	1	2.124	11.681	.002[a]
	Residual	6.182	34	.182		
	Total	8.306	35			

a. Predictors: (Constant), Do employees know IS policies

b. Dependent Variable: Have you been affected by Spamming

Figure 9c): Coefficient Model of Employee Know Policy and Spamming

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	T	Sig.
		B	Std. Error	Beta		
1	(Constant)	2.255	.271		8.322	.000
	Employees know IS policies	-.527	.154	-.506	-3.418	.002

a. Dependent Variable: Have you been affected by Spamming

Source: Research Data

4.1.4.6 Inadequate Training Influence on Identity Theft

Inadequate training correlates with Identity theft threats at R=.555 on Figure 10a) which is a high positive degree of correlation. Adjusted R square = 28.8% which means inadequate training can explain 28.8% of identity theft threats which is moderate. Since this model is P< 0.0005 which is less than 0.05 according to Figure 10b) implies that the model is good enough to predict the outcome of the variable. For every unit of increase in inadequate training, identity theft increases by 54.8% as shown by figure 10c).

Figure 10a): Model Summary of Inadequate Training influence and Identity Theft

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.555[a]	.308	.288	.422

a. Predictors: (Constant), Inadequate user training contribute to the security threats

Figure 10b): Anova Model of Inadequate Training and Identity Theft

ANOVA[b]

Model		Sum of Squares	Df	Mean Square	F	Sig.
1	Regression	2.694	1	2.694	15.127	.000[a]
	Residual	6.056	34	.178		
	Total	8.750	35			

a. Predictors: (Constant), Inadequate user training contribute to the security threats

b. Dependent Variable: Identity theft

Figure 10c): Coefficients Model of Inadequate Training and Identity Theft

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	.610	.219		2.785	.009
	Inadequate user training contribute to the security threats	.548	.141	.555	3.889	.000

a. Dependent Variable: Identity theft

Source: Research Data

4.1.4.7 Summary of Facilitating Factors with Spamming Threat

The various facilitating factors are regressed with spamming threats. R=.984 by Figure 11a) which is a very high positive degree of correlation. Adjusted R square = 95% which means the facilitating factors can explain 95% of spamming threats which is very high. Since this model is P< 0.0005 which is less than 0.05 according to Figure 11b) implies that the model is good enough to predict the outcome of the variable. From Figure 11c) for every unit of increase of employees knowledge in Information Security policies, it reduces spamming threats by 53.2% and this model is good enough to predict the outcome variable as P<0.0005 which is less than 0.05. Still from figure 11c) for every increase in unit of lack of IS security awareness there is a 28.1% decrease of spamming threat and this model is good enough to predict the outcome variable as P<0.005 which is less than 0.05. From the same figure, for every unit increase in usage of out dated software there is 25.8 increase in spamming threats and this model is good enough to predict the outcome of variable as P<0.005 which is less than 0.05. The other factors cannot be relied on to significantly affect spamming threat as P>0.005.

Figure 11a): Model Summary of Facilitating Factors and Spamming

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.984[a]	.967	.950	.109

a. Predictors: (Constant), Do employees scan flash disk, Lack of information system security awareness, Poor hosting of website, Weak Legislation , Poor IS selection, Do employees personal laptops and Ipads join the network, age bracket, access social media, Years at KRA, Inadequate user training, Outdated software, Do employees know IS policies

Figure 11b): Anova Model of facilitating factors and Spamming

ANOVA

Model		Sum of Squares	Df	Mean Square	F	Sig.
1	Regression	8.034	12	.670	56.711	.000[a]
	Residual	.272	23	.012		
	Total	8.306	35			

a. Predictors: (Constant), Do employees scan flash disk, Lack of information system security awareness, Poor hosting of website, Weak Legislation, Poor IS selection, Do employees personal laptops and Ipads join the network, age bracket, access social media, Years at KRA, Inadequate user training, outdated software, Do employees know IS policies

b. Dependent Variable: spamming

Figure 11c): Coefficients Model of facilitating factors and Spamming

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	2.804	.411		6.829	.000
	Inadequate user training	-.018	.060	-.019	-.295	.770
	age bracket	.008	.021	.023	.369	.716
	Years at KRA	-.059	.024	-.156	-2.427	.023
	access social media	-.161	.054	-.167	-3.006	.006
	employees know IS policies	-.532	.107	-.522	-4.979	.000
	Lack of IS security awareness	-.281	.075	-.269	-3.738	.001
	outdated software	.258	.073	.258	3.539	.002
	Poor hosting of website	-.084	.059	-.069	-1.416	.170
	Poor IS selection	-.027	.045	-.024	-.598	.556
	Weak Legislation	-.033	.048	-.033	-.693	.495
	Do employees personal laptops and Ipads join the network	.112	.058	.087	1.921	.067
	Do employees scan flash disk	.051	.044	.052	1.155	.260

a. Dependent Variable: spamming

4.1.5 Influence of Security Threats on E-Government Initiatives in KRA

4.1.5.1 Spamming Influence on ETR

Spamming correlates with ETR System KRA initiative at R=.567 as shown on Figure 12a) which is a very high positive degree of correlation. Adjusted R squared = 30.1% which means spamming can explain 30.1% of ETR system which is moderate. Since this model is P< 0.0005 which is less than 0.05 according to Figure 12b) implies that the model is good enough to predict the outcome of the variable. A single unit increment of spamming reduces ETR usage by 52.8% as shown by Figure 12c) means that spamming and ETR usage are indirectly proportional. The model is good enough to explain the outcome of the variable as p<0.0005 which is less than 0.05

Figure 12a): Model Summary of spamming influence on ETR

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.567[a]	.321	.301	.380

a. Predictors: (Constant), spamming

Figure 12b): Regression Model of Spamming influences on ETR

ANOVA[b]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	2.319	1	2.319	16.083	.000[a]
	Residual	4.903	34	.144		
	Total	7.222	35			

a. Predictors: (Constant), spamming

b. Dependent Variable: Do you use ETR

Figure 12c): Coefficients Model of Spamming on ETR

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	T	Sig.
		B	Std. Error	Beta		
1	(Constant)	2.441	.190		12.837	.000
	spamming	-.528	.132	-.567	-4.010	.000

a. Dependent Variable: Do you use ETR

Source: Research Data

4.1.5.2 Summary of Security Threats influence on ETR

Security threats correlates with ETR E-Government initiative at R=.819 as shown by Figure 13a) which is a very high positive degree of correlation. Adjusted R squared = 60.3% which means security threats can explain 60.3% of ETR system which is high. Since this model is P< 0.0005 which is less than 0.05 according to Figure 13b) implies that the model is good enough to predict the outcome of the variable. From Figure 13c) each unit increase of identity theft threat reduces ETR usage by 33.8% which means that identity theft and ETR usage are indirectly proportional. Also each unit increase of software bugs reduces ETR usage by 43.2%. The model is also good enough to predict the outcome of the variable as P<0.005 which is less than 0.05.

Figure 13a): Model Summary of Security Threats influence on ETR

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.819[a]	.671	.603	.286

a. Predictors: (Constant)
, computer virus, denial of service
, spamming, hacking, software bugs, Identity theft

Figure 13b): Anova Model of Security Threats on ETR

ANOVA[b]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	4.849	6	.808	9.876	.000[a]
	Residual	2.373	29	.082		
	Total	7.222	35			

a. Predictors: (Constant), computer virus, denial of service
, spamming, hacking, software bugs, Identity theft

b. Dependent Variable: Do you use ETR

Figure 13c): Coefficient of Correlation Summary of Security Threats influence on ETR

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	2.974	.450		6.608	.000
	spamming	-.318	.108	-.341	-2.936	.006
	hacking	-.165	.099	-.183	-1.665	.107
	Identity theft	-.338	.109	-.373	-3.094	.004
	denial of service	.177	.182	.109	.968	.341
	software bugs	-.432	.124	-.418	-3.500	.002
	computer virus	.078	.101	.087	.772	.446

a. Dependent Variable: Do you use ETR

Source: Research Data

CHAPTER FIVE: DISCUSSION, CONCLUSION AND RECOMMENDATION

5.1 Introduction

This study had the general objective of establishing the effect of security threats on e-government initiatives in the KRA. It also had three specific objectives. The first was to establish security threats on e-government initiatives in the KRA. Second was to establish the factors that facilitated security threats to e-government initiatives in KRA and lastly to determine the influence of security threats on e-government initiatives in the KRA.

5.2 Summary of Findings and Discussion

Majority of the respondents were between the age bracket of 26 to 30 and 31 to 35 years. This age group of young employees constituted 50% of the whole respondents. Age, however, is not a significant factor in determining security threats. The longer one has worked at KRA the less the chances of spamming threats by 28%. Thus the less one has worked is in the organisation, the higher their chance of encountering spam attacks. The data analysis reveals that at KRA software bugs at 25% are the most common threat followed by spamming at 21% and identity theft at 20%. Denial of Service threats was very minimal at 3%. Therefore a quarter of all threats in KRA are caused by software bugs. In terms of e-government initiatives, ITMS is the most used system by the respondents at 43% followed by Simba system at 41% and lastly ETR at 16%. ITMS and Simba systems have the most security threats especially software bugs and spamming. ETR has the least security threat. ETR unlike the other initiatives has computer virus as its major information security threat.

Employee usage of social media while at the office increases the chances of computer virus threats at 62%, however, social media is not significant in determining spamming threats. Out dated software increases the chance of getting software bugs by 45.2%. Out dated software is also significant in determining spamming attack. Each increase in usage of out dated software can increase spamming threats by 25.8%. Employees' knowledge of the Information System policies is significant in determining spamming threats. The

more knowledgeable employees are of Information System policies the more they may reduce spamming threats by 52.7%. Inadequate training is significant in determining identity theft. The more an employee is not trained, it increase the chances of identity theft by 54.8%. Inadequate training is, however, not significant in determining spamming attack at KRA.

Spamming threat attack is significant in determining usage of ETR system. Each unit of spamming threat reduces the usage of ETR by 52.8% which is quite high. This means that spamming threats and ETR usage are inversely proportional. Identity theft and software bugs are also significant in determining ETR usage. Each unit increase in identity theft reduces ETR usage by 33.8% while each unit increase in software bugs reduces ETR usage by 43.2%. Therefore in summary the significant factors influencing spamming threats are knowledge of Information Security policies, Information Systems security awareness and use of out dated software. ITMS and Simba system are the systems with the highest likelihood of security threats

5.3 Conclusion

From data analysis young employees were the majority of respondents while the more number of years one has worked at KRA reduces the chances of getting spamming threats. Software bugs, spamming and identity theft are the most common security threats at KRA while denial of service and computer viruses have the least effect. ITMS and Simba systems are the most used system by respondents who submitted their questionnaire. The two systems also faced the highest number of security threats especially software bugs and spamming. ETR had the least security threats and its major threat was from computer virus. Knowledge of information security policies, information systems security awareness and use of out dated software increase the likelihood of spamming attack. Inadequate training facilitates identity theft while out dated software facilitates software bugs from the data analysis. The security threats had a significant negative influence on ETR. Spamming threats, identity theft and software bugs each reduced the usage of ETR system.

5.4 Recommendation

E-Governance at KRA is affected by many security threats as evidenced in this study from the data analysis. KRA has to strive hard to ensure its IT systems especially the web based ones have the latest security systems in place to reduce exposure to the security threats. KRA is faced by major security threat from software bugs, spamming and identity theft. Software bugs are caused by not properly testing their systems before deployment hence hackers take advantage of the loopholes and steal information. KRA should embark on thoroughly testing of their systems especially ITMS and Simba before deployment to reduce the number of software bugs that exposes them to security threats. The system testing should be carried by a different group of people to ensure that the system complies with strict standards of security. For spamming KRA should install advanced spam filters and firewalls that block any fake mail from reaching them. For identity theft KRA should change the way they authenticate and authorise users. They may implement biometric systems and use feature like smart cards to identity users. They may also use higher encryption methods to ensure that data on transit cannot be spoofed by a hacker.

KRA employees should be properly and regularly trained on the software threats and how to mitigate them. The training should not just be for the IT people but encompass anyone who has access to a computer in the organisation. The Information security policy needs to be shared to all employees and be updated to include policy on posting government data on social media, scanning of flash disks and any other security tips. Out dated software including anti viruses needs to be updated regularly. KRA can install advance network management system that can track what each computer is doing and notify the administrators of the computers that have not updated their software. Since ITMS and Simba are the most used systems and most vulnerable systems to attack, they need to be closely monitored.

5.5 Limitation of the study

The study only covered KRA employees who work in IT department and are based in Nairobi. This was due to the time and logistics constraints. Some senior officers could not be reached due to them being in meetings usually outside their offices. If given more time

and resources the study could have covered a larger sample and revealed more about the subject matter.

5.6 Suggestions for Further Research

This research confirmed that there exist a lot of security challenges on e-government initiative at the KRA. Not all aspects of the security challenges and e-government initiatives were covered and calls for more study about them.

REFERENCE

Abrams, R. (2010, November 5). *Why is Unsecured WIFI So Risky?* Retrieved June 15, 2012, from http://blog.eset.com/2010/11/05/why-is-unsecured-wifi-so-risky

Alfawaz, S., May, L., & Mohanak, K. (2008). E-government security in developing countries:A managerial conceptual framework. *E-government and Institutional Change Journals*, 2-5.

Alsmadi, I. (2011, December). Security Challenges For Expanding E-governments' Services. *International Journal of Advanced Science and Technology, 37*, 47.

Andrews, D. P. (1999). National Security Telecommunications and Information Systems Security Committee. *National Information Systems Security(INFOSEC).*

Assange, J. (2006). *What is Wikileaks*. Retrieved June 13, 2012, from http://wikileaks.org/: http://wikileaks.org/

Ataya, G., Cuypers, J., Steven, H. D., Guldentops, E., Hardy, G., Koning, G., et al. (2006). Enterprise Value: Governance of IT investment. *The Business Case*, 2-3.

Backhouse, J. &. (2001). Current direction in IS security research: towards socio organizational perspectives. *Information Systems Journal, 11*(2), 128-130.

Bahadur, G. (2012). *What is Social Media Insecurity?* Retrieved July 25, 2012, from http://www.siliconindia.com/guestcontributor/guestarticle/327/What_is_Social_Media_Insecurity_Gary_Bahadur.html

Bell, & Greg. (2001). *Information Security Risk and Assessment, 2001 UNC Charlotte Symposium on Information Security and Privacy,*. Retrieved from http://www.sis.uncc.edu/LIISP/slides01/Greg-Bell.pdf

Bhattacharya, S., & Goswami, J. (2011). Study of E-Governance: The Attractive Way to Reach the Citizens. *IJCA Special Issue on "2nd National Conference- Computing, Communication and Sensor Network"*, 29-30.

Biztech Africa. (2011, October 29). *Safaricom unveils cloud deployment*. Retrieved October 29, 2011, from http://www.biztechafrica.com/section/internet/article/safaricom-unveils-largest-native-cloud-deployment-/1365/

CCK. (2012, April 17). *Communications Commision of Kenya*. Retrieved June 5, 2012, from http://www.cck.go.ke/news/2012/sector_statistics.html

Chandler, A. (1996). The Changing Definition and Image of Hackers in Popular Discourse. *International Journal of the Sociology of Law, 24*(2).

CISCO. (2011, December 14). *Cisco Connected World Technology Report*. Retrieved July 25, 2012, from http://www.cisco.com/en/US/netsol/ns1120/index.html#~2011,

Coleman, J. W. (2002). *The Criminal Elite: Understanding White-Collar Crime* (5 ed.). New York: Worth Publishers.

Conklin, A., & White, G. B. (2006). E-government and Cyber Security: The Role of Cyber Security exercises. *39th Hawaii International International Conference on Systems Science (HICSS-39 2006), CD-ROM / Abstracts Proceedings, 4-7 January 2006, Kauai, HI, USA* (pp. 79-87). IEEE Computer Society.

Duggal, P. (2011). *Cyberlaw an overview*. Retrieved June 6, 2012, from http://www.cyberlaws.net/cyberindia/articles.htm

Fallahi, M. (2007). *The obstacles and guidelines of establishing E-government in Iran.* MSc Thesis, Tarbiat Moddares University, Tehran.

Frank, D. (2003, January 27). Policy would secure users,transactions. *Federal Computer Week,Falls Church, 17*(2), 10.

Gartner Group. (2012). *E-Government*. Retrieved June 4, 2012, from http://www.gartner.com/technology/home.jsp

Gauci, M. (2008, October 23). *Computer Literacy Required in Employment*. Retrieved from http://www.infonet-ae.eu/en/news-items/computer-literacy-required-in-employment-0563

Gilmore, A., & D'Souza, C. (2006). Service excellence in e-governance issues: An Indian case study. *JOAAG, 1*(1), 2.

Grabosky, P., Smith, R., & Dempsey, G. (2001). *Electronic Theft: Unlawful Acquisition in Cyberspace.* Cambridge University Press.

Henriksson, A., Yi, Y., Frost, B., & Middleton, M. (2006). Evaluation instrument for e-government websites. *Electronic Government: an International Journal, 4*(2).

Hubbard, W. D. (2009). *The Failure of Risk Management: Why It's Broken and How to Fix It* (1 ed.). Wiley.

Humphreys, E. (2009). Implementing the ISO/IEC 27001—Information Security Management System Standard. *ISACA JOURNAL, 4*.

Hwang, M.-s., Li, C.-T., Shen, J. J., & Chu, Y.-P. (2004). Challenges of E-government and Security of information. *Information and Security: An international journal, 15*(1), 9.

Kanhere, V. (2009). Driving Value From Information Security: A Governance Perspective. *ISACA JOURNAL, 2*, 1.

Kaplan, A., & Michael, H. (2010). Users of the world, unite! The challenges and opportunities of Social Media. *Business Horizons, 53*(1), 59-68.

Kash, W. (2012, June 5). *Are Hackers Peering Through Your Laptop Webcam?* Retrieved June 15, 2012, from http://gov.aol.com/2012/06/05/are-hackers-peering-through-your-laptop-webcam/

Kemibaro, M. (2011, October). *SafaricomCLOUD: Safaricom's third act to dominate Kenya's telecoms sector?* Retrieved August 21, 2012, from http://www.moseskemibaro.com/2011/10/29/safaricomcloud-safaricoms-third-act-to-dominate-kenyas-telecoms-sector/

Kessler, K., Hettich, N., Parsons, C., Richardson, C., & Triana, A. (2011). A Framework for Assessing Privacy Readiness of e-Government. *iGovernment, 21*.

KRA. (2011). *KRA Online Services*. Retrieved June 5, 2012, from http://www.kra.go.ke/index.php/kra-portal

Langenderfer, J., & Miyazaki, A. (2009). Privacy in the information economy. *Journal of Consumer Affairs*, 380.

Longe, O. (2004). *Proprietary Software Protection and Copyright issues in contemporary Information Technology.* M.Sc Thesis (Unpublished), Federal University of Technology, Akure.

Lyambila, T. (2010). *UK Kenyans told to embrace Konza*. Retrieved June 4, 2012, from http://www.kenyalondonnews.co.uk/index.php?option=com_content&view=article&id=9542:uk-kenyans-told-to-embrace-konza&catid=73:kenya-diaspora&Itemid=61

Madowo, L. (2011, January 4). *Hacker Defaces Website Of Kenya*. Retrieved August 21, 2012, from http://techcrunch.com/2011/01/04/hacker-defaces-website-of-kenya-police-in-tribute-of-mark-zuckerberg/

Makatiani, W. (2012). *Information Intelligence and Analytics*. Retrieved June 14, 2012, from http://serianu.com

Marete, G. (2011, June 5). *Aeromarine*. Retrieved September 13, 2012, from http://www.aeromarine.co.ke

Mbuvi, D. (2012, January 17). *103 Government of Kenya websites hacked overnight*. Retrieved June 5, 2012, from http://www.cio.co.ke/news/main-stories/103-Government-of-Kenya-websites-hacked-overnight

Mugenda, A. G. (2008). *Applied Research and Training. Nairobi, Kenya.* Nairobi: Applied Research and Training Services.

Mutegi, M. (2011, August 11). *New date for ICT park takeoff*. Retrieved August 11, 2011, from http://www.nation.co.ke

N, E. (2003). *nformation Security Guideline for NSW Government – Part 1 Information Security Risk Management*. Retrieved August 21, 2012, from www.oict.nsw.gov.au/pdf/4.4.16.IS1.pdf

Ndou, V. (2004). E-government for developing countries: Opportunities and challenges. *The Electronic Journal on Information Systems in Developing Countries*.

Nikkhahan, B., Aghdam, A. J., & Sohrabi, S. (2009, April). E-government security: A honeynet approach. *International Journal of Advanced Science and Technology, 5*, 75.

Ochara, N. M. (2008). Emergence of the E-Government Artifact in an Environment of Social Exclusion in Kenya. *The African Journal of Information Systems, 1*(1), 18.

Oliver, D., Allard, J.-L., Antonsson, E., Bahl, S., Brotby, K. W., Dimitriadis, C., et al. (2009). The business model for information security. *ISACA*, 5.

Omwansa, T. (2009). M-PESA: Progress and Prospects. *innovations / Mobile World Congress*, (p. 108).

Ransome, J. W. (2009). *Cloud Security Challenges*. Retrieved from http://www.infosectoday.com/Articles/Cloud_Security_Challenges.htm

Safaricom. (2011, October). Retrieved 2011, from Cloud Computing: http://www.safaricom.co.ke/index.php?id=413

Schwester, R. W. (2009). Examining the Barriers to e-Government Adoption. *Electronic Journal of e-Government, 7*(1).

Scott, R. (2003). Planners need to plan for disaster. *Accounting Today, New York*, 18-20.

Sembok, T. T. (2003). *Ethics of Information Communication Technology (ICT).* Universiti Kebangsaan Malaysia, Bangkok.

Smith, S., & Jamieson, R. (2006). Determining key factors in E-Government information security systems. *Information systems management spring*, 23.

Stibbe, M. (2005). E-government security, Infosecurity Today. *Stibbe, M*, 8-10.

The World Bank Group. (2011). *The World Bank*. Retrieved June 4, 2012, from http://web.worldbank.org/WBSITE/EXTERNAL/TOPICS/EXTINFORMATIONANDCOMMUNICATIONANDTECHNOLOGIES/EXTEGOVERNMENT/0,,contentMDK:20507153~menuPK:702592~pagePK:148956~piPK:216618~theSitePK:702586,00.html

Wanjiku R. (2009). *Kenya Communications Amendment Act (2009) - Progressive or Retrogressive?* Retrieved from Association for Progressive Communications [Online: http://www.apc.org/en/system/files/CICEWAKenya20090908_EN.pdf

Wanjiku, R. (2010, June 23). *East Africa countries favor ICT sector in budgets*. Retrieved June 5, 2012, from http://www.computerworld.co.ke/articles/2010/06/23/east-africa-countries-favor-ict-sector-budgets

Yang, C. (2008). *Intelligence and Security Informatics* (1 ed.). Springer.

Yar, M. (2006). *Cybercrime and Society.* SAGE Publications Ltd.

APPENDICE

APPENDIX I: Questionnaire

I am carrying a research on the Information security threats and e-government initiatives in the Kenya Revenue Authority (KRA). I would like to hear your views on this. I hope that you will respond to all of the questions. The information you provide will be used for research purposes only and will be treated with the privacy and confidentiality it deserves. None of the information will be disclosed to any authority nor the identity of the respondent revealed. If you would like to have a question clarified, feel free to ask. Your responses will be highly confidential thank you.

Section A: Demographic data

1. Age group

   ☐ <= 25 years ☐ 26 to 30 years

   ☐ 31 to 35 years ☐ 36 to 40 years

   ☐ 41 to 45 years ☐ Above 46 years

2. Designation/Position …….....

3. Highest level of education

   ☐ Certificate ☐ Diploma

   ☐ Undergraduate Degree ☐ Postgraduate Degree

4. Other professional qualifications and computer training…….....

5. Years employed at the Kenya Revenue Authority

☐ <= 5 months ☐ 6 months to 1 year

☐ 2 to 5 years ☐ 6 to 10 years

☐ 11 to 20 years ☐ Above 21 years

6. Which information systems do you interact with (Check all that you use)

☐ Simba system ☐ ITMS

☐ ETR ☐ Others

A. If you selected **Others** above please specify them……

Section B: Information Security threats

1. Have there been any information security threats to your systems

☐ Yes ☐ No

2. What security threats have affected your systems (Check all that have affected you)

☐ Spamming ☐ Hacking

☐ Identity theft ☐ Software bugs

☐ Computer Viruses ☐ Denial of service attack

☐ Others

A. If you selected **Others** above please list them……

3. How severe have the threats impacted your systems

Threats	**Never affected**	**Very weak**	**Weak**	**Strong**	**Very Strong**
Spamming					
Hacking					
Identity theft					
Software bugs					
Computer Viruses					
Denial of service attack					
Malware attack					
Others					

4. How often have you been attacked by these threats

Threats	**Never**	**Very Rarely**	**Rarely**	**Often**	**Very Often**
Spamming					
Hacking					
Identity theft					
Software bugs					
Computer Viruses					
Denial of service attack					
Malware attack					
Others					

Section C: Factors that Facilitate Information Security Threats

1. Factors which may have contributed to security threats to Kenya Revenue Authority Information Systems

Issues	**Yes**	**No**
Lack of information system security awareness		
Poor information systems selection		
Weak Legislation		
Inadequate user training		
Out dated software		
Computer viruses		
Poor hosting of websites		
Others		

2. Information Security awareness

Issues	**Yes**	**No**	**Explanation**
Do your fellow employees know the information security policies?			
Are your fellow employees allowed access to social sites in the office?			
Do you have a policy on posting government data on social media?			
Do employees scan flash disks and CDs when inserting them on the computer?			
Are personal laptops/ipads allowed to join the organisation network?			