Assessment of Effect of Information System Security Threats on Information Resources in Public Institutions: A Case of Kenya School of Government

Emma Jepkemboi Kemei, Dr. James Ogalo, Prof. Kibiwott Kurgat
Faculty of Information Science and Technology Kisii University
Faculty of Information Science and Technology Kisii University
Faculty of Information Science and Technology Kisii University
Corresponding author: Emma Jepkemboi Kemei

Abstract: *Information system security is important in an institution whose routine operations expose its information system to threats. The objectives of the study were to establish the effect of systems security threats on the utilization of information resources and to find out the challenges of information system threats on organizational information resources in Kenya School of Government. The study employed the descriptive survey research design. The study targeted 100 staff drawn from the ICT Department, secretarial and records departments. Census sampling was employed to select the sample size. Data was collected using self administered questionnaires and analyzed using descriptive statistics with the aid of Microsoft Excel. The findings were presented using tables and graphs. From the results, it was evident that there were widespread systems security threats on the utilization of information resources at the Kenya School of Government, with the illegal access to computer system being the highest and computer related acts causing personal harm being the lowest. The findings also indicate that the organizations have not embraced ICT policies and strategies to help secure their systems. However, organizational commitment to curb cybercrime was high which may be attributed to e-government requirements like e-procurement and IFMIS which must be carried out online. The study also established that cost was the highest challenge in adopting and implementing ISS.*

Keywords: *Computer security policy, Computer Security, E-government, Information security strategy implementation, Information System Security Threat, Information system, Policy, Public Organization, Security breach, System integrity, Threat*

Date of Submission: 31-08-2017 Date of acceptance: 07-11-2017

I. Introduction

Information technology is globally acknowledged as the engine that drives economies of countries in the world. It enables the government to provide better services to its citizens and to improve economic productivity (NIST, 2011). Quite a number of organizations depend exclusively on information systems to successfully undertake their mandate. As a result of the remarkable progress made in the development, adoption and utilization of information technology, it has become necessary to adopt measures that cushion all concerned institutions against any kind of threats. This is because the new technology is not immuned to roving cyber-threats. Safety measures against information systems threat is important particularly in the public sector which serves as a large data base for the government. Therefore, all government institutions should become responsible and accountable in managing threats to information systems. Information systems security addresses not just data but the dynamic transformational contexts in which the data is applied (Gurpreet & James, 2000).

Owing to the sensitivity of government data, interest in information security has become a mundane issue as reflected in the current standards and certifications on internet security (Whiteman & Mattrod, 2003). According to Bobert and Kenneth (2009) the security of information systems for government institutions is important because such institutions are the targets of cyber-crime. In terms of financial security, it is important to protect institutions from system threats that could negatively impact on organizations' finances. However, the speed at which technology is evolving makes it difficult to provide reliable protection. In Britain, Grimson (2005) reported that advancements in technology and the need for reliable data networks has fostered a desire to efficiently make use of computing resources for the safety of all users. Compared to other countries, Kenyan government relies on common IT platforms and new technologies to increase efficiency and effectiveness of government services. According to Obure (2002) IT has facilitated communication in all government institutions. However, these technologies present threats that pause major security threats. Thus, there was need to find out how the government is securing the cyberspace from information system threats.

1.2 Problem Statement

Most public institutions usually collect and store large volume of vital information and transmit data across distributed network of computers (Katundu, 2014). However, there is an increasing volume of complicated cyber-attacks on such data. For instance, in 2013, 103 government websites were defaced while in 2014 websites and government twitter accounts were hacked. Since users pause a major threat to information system security, there is need to understand the risk they pause to data held in information resources. Although, information management influences the perceptions of threats, there is need to understand the effect of the threat to information security on an organization's information resources (Gurpreet, 1995). Previous studies have addressed computer security generally, but there are few studies conducted that have addressed the issue of information system security threats in public organizations in Kenya. The study sought to assess the effects of information system security threats on information resources in public institutions in Kenya.

1.3 Objectives of Study

i. To establish the effect of the information system security threats on the utilization of information resources at the Kenya School of Government.

ii. To find out the challenges of information system threats on information resources at the Kenya School of Government.

II. Literature Review

2.1 Information System Security Threats

The advancement in information and communication technologies has facilitated the presence of enormous and vast amounts of information. This has also generated significant risks to computer systems and to other critical operations and infrastructures they support. In spite of the significant advances in information security, many information systems are still vulnerable to inside or outside attacks that inflict various types of damage resulting in enormous losses (Ana-Maria, Mihai & Florin, 2010). This damage can range from human errors to unprecedented accidents destroying entire computer centers. Losses can stem from the actions of supposedly trusted employees defrauding a system, hackers and crackers, or from careless data entry clerks. According to Barbara and Edward (1995) threats to information systems and cyber-based critical infrastructures are evolving and growing. These threats come from a variety of sources such as foreign nations engaged in espionage and information warfare, criminals, hackers, virus writers and disgruntled employees and contractors working within an organization (Gregory, 2009). According to Vijay (2013) disastrous but prevalent information security control deficiencies continue to place public IS's at risk by inadvertent or deliberate misuse, unauthorized modification or destruction, inappropriate disclosure and critical operations disruption. An underlying cause for all these weaknesses is that organizations need to effectively transform key elements of their vast information security programs. These consequences have been experienced in many institutions all over the world including Kenya where negative impact has been felt.

2.2 Strategies employed on Information Resources security

The structure of cyber attacks response differs from one state to another, and some countries have cyber crisis management systems that put defense and damage restoration above cyber attacks attribution. By doing so, it becomes extremely difficult not only in the attribution of a certain cyber attack, but also in generating information about the varying nature of threats, the characteristics and methodologies of threats and emerging threat idiosyncrasies for the purpose of developing response strategies and reallocating resources, as necessary, to accomplish effective prevention (Carter & Schafer, 2005). A key aspect in IS management involves organization's context, where the occurrence is deployed and operates. Each organization has its unique setting and constraints such as political, social and economic ones. Ultimately these constraints can impose different issues relevant to ISs management.

Most researchers recommend that in an environment of government initiatives and low level of ICT readiness, there would be less emphasis on privacy, security and confidentiality issues (Nour, 2007). Therefore, it is important to gain understanding of the organizational and national dimensions in which the organization operates. Computer systems often critically support the mission of an organization. Protecting them can be as critical as protecting other organizational resources such as money, physical assets or employees. However, incorporating security considerations in the management of information and computers does not completely eliminate the possibility that these assets will be harmed. Ultimately, organizations have to decide what the level of risk they are willing to accept, taking into account the cost of security controls. As with other resources, the management of information and computers often transcend organizational boundaries. When an organization's information and computer systems are linked with external systems, management's responsibility also extends beyond the business. This requires that the management understands the general level of security employed on the external systems or seek assurance that the external system will provide adequate security to the organizational data (Molla & Ioannis, 2005). Securing information has become an important function within the

IS management regime. Effective guidelines for IS security also guarantee organizations' privacy, veracity and accessibility of information. Issues related to public sector management require more consideration of organizational environment, culture and stakeholders. Despite increasing investment in information security and its strategic role in organization's success, effective implementation of information security strategy still remains one of the top challenges facing global organizations (Ernst & Young, 2008; Fratto, 2009). In order to take advantage of new opportunities brought by information technology advances, Caralli (2004) suggests organizations should shift the focus from a technology-based information security strategy to an organizational-based approach that considers a core set of organizational capabilities. Therefore, identification and understanding of organizational capabilities is essential to logically recognize the relationship between information security strategy implementation success and organization performance.

2.3 Challenges Information System Security Threats pose in Organizational Performance

Organizations involved in governance are reliant on a continuous assortment of data management systems and technologies that enable them to improve efficiency in service delivery (Ernest & Young, 2013). Most of the basic services offered by many organizations such as registration, advertisements and online transmission of tax returns are some of the major activities currently undertaken through e-government initiative. This has necessitated reliant on distributed systems across the globe. However, managing risks associated with government's growing dependence on information technology is obviously a continuing challenge; a balancing act between maintaining security and not inhibiting the business (Eric & Goetz, 2007). Due to the high-profile organizational failures of the past decade, legislatures, statutory authorities and regulators have created a complex array of new laws and regulations designed to force improvement in organizational governance, security, controls and transparency. Previous and new laws on information retention and privacy, coupled with significant threats of information systems disruptions from hackers, viruses and terrorists, have resulted in a need for a governance approach to information management, protecting the organization's most critical assets, its information and reputation. Information security is thus especially important for organizations to ensure the confidentiality, integrity and availability of information and information systems. Conversely, ineffective information security controls can result in significant risk to a broad array of government operations and assets (Gregory, 2009).

According to Baker (2015) all organisations are vulnerable to attack and no security system is completely immune. The level of vulnerability, though, depends on many factors, such as the industry and geographies in which that organisation operates, the nature of the business it conducts, the adequacy of its technology and security systems, processes and procedures, internal compliance with established processes and its public profile and supply chain. In the USA for instance, frequent cyber-attacks have had devastating impact on government operations (Robert, 2014). In Africa, governments are facing unprecedented level of cyber-attacks and many businesses that store confidential customer and client information online are presented with a struggle to maintain their reputations in the wake of massive data breaches (Frost & Sullivan, 2015).

III. Methodology

The study was based on a descriptive survey design. The study targeted departments offering IT and related services which included the ICT department, secretaries and registry department at the Kenya School of Government Headquarters in Nairobi and its constituent campuses namely Kabete, Embu, Baringo, Matuga and Mombasa. The target population was 100 staff working in the ICT Department, secretaries and records officers. The study employed the use of census method and the entire population was included in the study. The sample size of the study included all the target population in the six campuses totaling to 100. Data was collected using a semi-structured questionnaire. The questionnaire was deemed fit for data collection on account of its ability to give respondents an opportunity to express themselves on key issues in their day to day encounters. To ensure reliability of the instrument, the researcher first conducted a pilot test using 10 questionnaires. Based on the subjective opinion of the supervisors, modification of each and every question was done until the researcher was sure that it provided an accurate measure. Before undertaking the study a number of safeguards were ensured. For instance, the researcher sought permission from the relevant authorities to allow data collection. In addition, the researcher took all the reasonable measures to protect the respondents physically and psychologically. The findings and interpretations are honest and objectively presented to avoid untrue, deceptive and doctored results. The analysis of the research data proceeded through four major steps: data cleaning or editing; coding; tabulations; and interpretation of results (Collis & Hussey, 2003; Obure, 2002). Data analysis was carried out with the aid of the Microsoft Excel. Data was presented using tables and graphs.

IV. Results and Discussion

4.1 Common Threats

The researcher sought to establish the level of unlawful access to computer system and the results are presented in table 1.

Table 1: Level of illegal access to computer system

Rate of illegal access to computer system	%
Very high	14
High	32
Moderate	24
Low	17
Very Low	6
Negligible	8
Total	100

Majority (32%) of the respondents' contented that the level of illegal access to computer system was high, whereas 14% agreed that the threat was very high and 24% responded as moderate. This brings to a total of 70% (very high, high and moderate) response that there was illegal access to computer system in the organization. This brings attention to the organizations' ICT personnel to ensure that safeguards are formulated to curb the threat. The rest of the respondents agreed that there was low threat at 17% and very low 6%. Moreover, the researcher asked the respondents to evaluate the level of prohibited interception, access or acquisition of Computer Data. The findings are presented in tale 2.

Table 2: Level of prohibited Interception, interruption or access of computer data

Rate of Prohibited access, interception or acquisition of computer	%
Very high	17
High	25
Moderate	21
Low	21
Very Low	13
Negligible	4
Total	100

As shown in table 2, 17% of the respondents revealed that the level of prohibited, interception or access of information was very high, whereas 25% said that the threat was high, and 21% pointed out that the level was moderate. This resulted to a total of 63% response which is higher than normal. This rate is dangerous for the safety of the crucial data in the organization, thus calling for strict measures to all personnel to ensure that data is kept safe and confidential at all times. Further, 21% accepted that the threat was low; another 13% also accepted that the threat was very low. The results in table 3 show the level of illegal data interference or system interference.

Table 3: Illegal data interference or system interference

Rate of illegal data interference or system interference	%
Very high	19
High	21
Moderate	19
Low	24
Very Low	11
Negligible	6
Total	100

Majority (24%) of the respondents noted that illegal interference threat was low, whereas 19% agreed that the threat was very high, while 21% agreed that the threat was relatively high. The rest agreed that the threat was very low at 11% and negligible at 6%. Although majority agreed that the threat was low, a worrying 59% agreed that the there was illegal data interference. This also calls for all the respective personnel to put in place measures o ensure that data integrity is maintained and all aspects of their IS system is always secured from illegal interference. The level of breach of measures instituted to protect data was also sought as shown in table 4.

Table 4: Level of breach of measures of data protection

Rate of breach of privacy or data protection measures	%
Very high	22
High	22
Moderate	23
Low	11
Very Low	15
Negligible	8
Total	100

It is evident that 22% each of the respondents contented that the threat was very high and high while 23% agreed that the threat was moderate. This totals to a 67% response that the threat was higher. This poses a threat to organization's private data whose accessibility may be a reserve to only few individuals. Therefore, the organization should be able to use these findings and enlighten their staff on issues of emerging data safety and privacy in the market. Whereas 11% agreed that the threat was low, the remaining 15% and 8% contented that the threat was very low and negligible respectively. The results on the level of computer fraud or forgery are presented in table 5.

Table 5: Level of computer fraud or forgery

Rate of computer related fraud or forgery	%
Very high	13
High	17
Moderate	14
Low	27
Very Low	14
Negligible	15
Total	100

Majority (27%) of the respondents agreed that the level of computer fraud or forgery was low while 13% contented that the threat was very high with 17% of the respondents agreeing that the threat was high. 14% of the respondents accepted that the threat was moderate while the remaining 14% and 15% contented that the threat was very low and negligible respectively. A total of 54% of respondents agreed that computer related fraud and forgery also existed in their organization. This calls for the organization to introduce a method for vigilant verification of important documents generated for use by staff, customers and other stakeholders in the organization. The researcher also sought to ascertain level of offences related to computer copyright and trademark and the findings are presented in table 6.

Table 6: Level of offences related to computer copyright and trademark

Level of measurement	%
Very high	15
High	18
Moderate	27
Low	21
Very Low	4
Negligible	14
Total	100

Majority (27%) of the respondents contented that the threat of computer related copyright and trademark offences was moderate. Moreover, 15% agreed that the threat was very high while 18% agreed that the threat was high. This represents a 60% response rate which confirms that in relation to copyright and trademark offences existed. This serves as benchmark for the organization to adopt modern measures to curb these offences. The results in relation to sending or controlling spam are presented in table 7.

Table 7: Level of sending or controlling spam

Level	**%**
Very high	7
High	24
Moderate	27
Low	27
Very Low	4
Negligible	11
Total	100

When asked about the threat level of sending or controlling spam, 7% of the respondents contented that the threat is very high, while 24% agreed that the threat is high, another 27% agreed that the threat is moderate. This a total of 58% agreed that the threat of spam exists in their system, this brings to the attention of the ICT department to put up control measures to ensure that each mail and message received is first filtered before it gets into the system. Another 27% agreed that the threat is low, whereas 4% responded as very low and the remainder 11% agreed that the threat is negligible.

Table 8: Level of personal harm that relate to computer

Level of Rating	%
Very high	7
High	19
Moderate	14
Low	27
Very Low	13
Negligible	20
Total	100

In regard to the level of threat posed by computer based crimes causing personal harm, 7% of the respondents agreed that the threat is very high, while another 19% agreed that the threat is high, while 14% agreed that the threat is moderate. This brings to a total of 40% response that the threat exists. Further, 27% of the respondents contented that the threat was low; while the remainder 13% and 20% contented that the threat was low and negligible respectively. This brings to the attention of the organization to ensure they put in place measures that the users of their ISs are protected against any harm caused by sex.

Table 9: Level of computer related to creation and dissemination of child pornography

Rate	%
Very high	16
High	14
Moderate	16
Low	19
Very Low	17
Negligible	19
Total	100

When asked about the level of threat posed by computer related creation and dissemination of child pornography, 16% of the respondents contented that the threat is very high, while 14% agreed that the threat is high and 16% agreed that the threat is moderate. This is a total of 46% response; this may be attributed to the fact that there is an increase of children having access to ICT and related gadgets. Control measures should be strictly put in place by all the stakeholders to guarantee that children are excluded from harmful cyber threats and pornography. 19% of the respondents agreed that the threat is low, 17% and 19% agreed that the threat is very low and negligible respectively.

Table 10: Level of computer acts associated with acts in support of terrorism offences

Rate	%
Very high	14
High	16
Moderate	11
Low	10
Very Low	17
Negligible	31
Total	100

Majority (31%) of the respondents contented that the threat of computer associated acts that appear to support terrorism is negligible in the organization. Although, a total of 41% contented with the fact that the threat exists that is 14% of the respondents agreed that the threat is very high, while 16% agreed that the threat is high and 11% agreed that the threat is moderate. Currently, terrorism has been a major threat to both national security and worldwide, this problem is perpetrated by widespread internet accessibility, which enables faster communication. The remaining 17% agreed that the threat is very low. Illegal access is rated as the highest ISS threat with 70% response; other threats which had a high response rate were breach of secrecy, unlawful admittance, disruption or procurement of computer data and copyright and trademark offences with 67%, 63% and 60% respectively. The ISS threat which were rated lowest was computer related acts causing personal harm at 40%. Other types of cybercrimes experienced in the organization included scams, potentially unwanted programs, maladvertising, social engineering, hacking and cracking, plagiarism, identity theft, cyber stalking, hardware failures and data IISs, denial of service and child soliciting and abuse.

4.2 Challenges facing Adoption of ICT

In regard to the challenges facing implementation of ICT, the respondents were first asked to rate some factors which important in their planning for ICT security. These factors were subdivided into four categories; cost, value, difficulty and company's needs.

Table 11: Cost effect in planning and adoption of ICT

Rate of importance	%
Highly important	23
Very important	26
Important	22
Less important	22
Not important	8
Total	100

When asked about the level of importance of cost of planning and adopting ICT in their organization, majority (71%) of the respondents concurs that the cost was an important factor with 23% of the respondents agree that the cost factor is highly important when planning for ICT security, 26% contented that it is very important, while 22% agreed that it is important. This requires adequate budget allocation for ICT services to enable them utilize ICT resources effectively. The remaining 22% and 8% agreed that cost is less important and not important respectively.

Table 12: Value of ICT

Rate of importance	%
Highly important	5
Very important	27
Important	14
Less important	27
Not important	27
Total	100

When asked to rate the value ICT planning and adoption will add to their organization, 5% of the respondents agree that it is highly important, 27% agree that is very important, while 14% agree that it is important. This presents a 46% acceptance that planning and adoption of ICT is important to the organization. The remaining 55% responded as less important and not important respectively.

Table 13: Difficulty in ICT usage

Rate	%
Highly important	10
Very important	16
Important	29
Less important	27
Not important	19
Total	100

On matters of learning on how to adopt and use ICT, 10% of the respondents agreed that ICT is difficult and expensive to use, 16% agree that it is important, while 29% content that it is important. This presents a 54% response that ICT is indeed difficult and expensive to use; this may be explained by the fact that ICT usage requires prior training in its usage which has cost implications to the user. The remaining 27% and 19% responded as less important and not important respectively. It is not meeting the company's needs.

Table 14: Company's needs

Rate	%
Highly important	8
Very important	17
Important	27
Less important	21
Not important	27
Total	100

When asked about the, importance of ICT in meeting their company's needs, majority (52%) of the respondents agree that ICT is important with 8% respondents agree that it is highly important, 17% agree that it is very important and 27% agree that it is important. The remainder 48% content that it is less important and not important respectively. The researcher also sought to ascertain whether ICT and business operations improvement as presented in table 15.

Table 15: ICT and business operations improvement

Response	%
YES	79
NO	21
Total	100

When asked if ICT improves their business operations in their organization, large proportion (79%) of the respondents agree that ICT adoption in their organization improves their business operation. This is may be attributed e-government initiatives on automation of most of the operations in organizations. The remaining 21% contented that ICT does not improve their operations.

V. Conclusion

The findings indicate that most of ISS threats were many with prohibited access to computer system being the major threat to information resources in public institutions in Kenya. Also, breach of privacy, prohibited access and interception of data and computer related copyright and trademark offences affected information resources in public institutions in Kenya. These threats may be attributed to the fact that most ISS in the organization have a shared common password which enable colleagues to access another person's computer over LAN. Other ISS threats are illegal data interference, spam, identity offences linked to computer, child pornography, computer related fraud or forgery, acts associated with computer involving racism or xenophobia, acts linked to computer but are described as acts bordering on terrorism and computer related acts causing personal harm. Most of these threats are internet related contributed by the fact that there is open access to internet across all the organization's premises. Other threats included harms scams, potentially unwanted programs, maladvertising, social engineering, plagiarism, identity theft, cyber stalking, hardware failures and data IISs, denial of service and child soliciting and abuse.

The study ha also revealed that cost was the major challenge facing the adoption of ICT as procurement of ICT combines several entities ranging from hardware, software, peripherals, training of users among others all of which are expensive and funds are always limited. This problem may be solved by increasing the budgetary allocation to ICT annually. Other challenges included value of ICT to the organization. ICT is difficult and ICT not meeting the company's needs. This was attributed to the fact that ICT requires skilled personnel. Technicality of ICT is noted as the greatest barrier to adoption in ICT thereby presenting an opportunity for the organization to ensure that staff are computer literate in order to embrace ICT fully. Policies, level of access and cost were other challenges hindering adoption of ICT.

From the research findings ISS threats are widespread and their management is still wanting as the organization have challenges understanding and managing these threats. There is inadequate organizational commitment to ICT at Kenya school of government. Poor planning on ICT is also a contributing factor because it borders on issues to do with adequate budget allocation, staff recruitment and training. Another major challenge facing adoption of ICT is the issue of change management where people are slow to upgrade their ISS to curb cyber threats which evolve daily.

References

[1] Ana-Maria, S., Mihai, B. & Florin, G. (2010). Audit for Information Systems Security, Information Economica vol. 14, no. 1.

[2] Baker, B. (2015). The Future of Cyber-Security-Threats and Opportunities, Global Corporate Venturing,

[3] Barbara, G. & Edward, A. (1995). An Introduction to Computer Security: The NIST Handbook, NIST Special Publication 800=12, US Department of Commerce, USA.

[4] Bobert, S. & Kenneth, K. (2009). Local government IT Implementation issues: a challenge for public administration, Hawaii International Conference on System Sciences, Hawaii, USA.

[5] Caralli, R. A. (2004). Managing for Enterprise Security, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA.

[6] Carter, D. L., & Schafer, J. A. (2005). The Future of Law Enforcement Intelligence. In J. A. Schafer (Ed.), Policing 2020:Exploring the Future of Crime, Communities, and Policing: Police Futurists International. p. 235.

[7] Collis, C. C. & Hussey, S. C. (2003). Mitigating information security risks By increasing user awareness: A case study of information security awareness system. Information Technology, Learning & Performance Journal, 24, 1-14.

[8] Eric J. & Goetz, E. (2007). Embedding Information Security into the Organization, Managing Organization Security, IEEE Computer Society, Texas, US.

[9] Ernest and Young (2013). Building a Better Working World, EYGM Limited, UK, October 2013

[10] Fratto, P. (2009). Certifying Information Security Management Systems, Information Security Corporation.

[11] Frost, W. & Sullivan, P. (2015).The 2015 Global Information Security Workforce Study, PDF.

[12] Gregory, C. W. (2009). Cyber Threats and Vulnerabilities Place Federal Systems at Risk, United States Government Accountability Office, Washington D.C.

[13] Grimson, A. (2005). Do IT Investments a Real Business Value?, Applied Informatics, No.4, pp. 180-189.Washington DC, US.

[14] Gurpreet D. & James, B. (2000). Information System Security Management in the New Millenium, Communications of the ACM.

[15] Gurpreet, D. S. (1995). Interpreting the management of Information SystemsSecurity, Department of Information Systems, London School of Economics and Political Science, Houghton Street, London

[16] Katundu, N. (2014). Enterprise Vulnerability Management and Its Role in Information Security Management, Information System Security 14(3):29-56.

[17] Molla, K. & Ioannis, K. (2005). Overview of Kenya's Cybersecurity Framework, ITU Workshop on "ICT Security Standardization for Developing Countries, Geneva, Switzerland.

[18] NIST (2011). Managing Information Security Risk: Organization, Mission and Information System Review, Joint Task Force Transformation Initiative, Computer Security Division, Information Technology Laboratory, NIST, Gaithersburg, MD 20899-8930, USA.

[19] Nour, M. (2007). A Context-based Integrative Framework for e-government Initiatives, Government Information Quarterly, 25(3):448-46

[20] Obure, J. M. (2002). Handbook on Data Analysis Using SPSS Version 10.0. Nairobi: M & O Data Experts and Training Consultants

[21] Robert, P. (2014). Cyber Risks: The Growing Threat, Insurance Information Institute, UK.

[22] Vijay, G. (2013). Information System Misuse: Threats and Counter Measures, Riyadh, Saudi Arabia, 2006

[23] Whiteman, M. E., & Mattrod, H. L. (2003). Principles of Information Security, Thomson Learning, Boston: Academic Press.

Emma Jepkemboi Kemei Assessment of Effect of Information System Security Threats on Information Resources in Public Institutions: A Case of Kenya School of Government." IOSR Journal of Computer Engineering (IOSR-JCE) , vol. 19, no. 6, 2017, pp. 25-33