Asian Journal of Research in Computer Science

2(1): 1-11, 2018; Article no.AJRCOS.45049

Facilitating Factors for Cybersecurity Vulnerabilities in Kenyan County Governments

Kadima Victor Chitechi[1*], Samuel Mbugua[2] and Kelvin Omieno[1]

[1]Masinde Muliro University of Science and Technology, Kenya.
[2]Kibabii University, Kenya.

Authors' contributions

This paper was carried out in collaboration between all authors. Author KVC designed the study, collected data, literature searches, performed the statistical analysis, discussed findings and wrote the first draft of the manuscript. Authors SM and KO managed the editorial of the study. All authors read and approved the final manuscript.

Article Information

DOI: 10.9734/AJRCOS/2018/45049
Editor(s):
(1) Dr. Stephen Mugisha Akandwanaho, Department of Information Systems and Technology, University of KwaZulu-Natal, South Africa.
Reviewers:
(1) Jose Ramon Coz Fernandez, University Complutense of Madrid, Spain.
(2) Idrees S. Hussein, Duhok Polytechnic University, Iraq.
Complete Peer review History: http://www.sciencedomain.org/review-history/27215

Original Research Article

Received 26 August 2018
Accepted 07 November 2018
Published 14 November 2018

ABSTRACT

Globally, ICT is regarded as a driver and enabler; thus, organisations which have integrated ICT in their systems have had immense growth and output. The adoption of ICT into the Kenyan County Governments, therefore, promises equal growth and output. These benefits notwithstanding, integration of ICT systems into County Governments is faced with a number of challenges in terms of vulnerabilities and other cybersecurity risks. This paper sought to identify the key facilitators of cybersecurity vulnerabilities in Kenyan County Governments only. The exploratory research design was used as a methodology. Questionnaires and interview schedules were the main instruments of data collection. The data was analysed using descriptive and inferential statistics. The findings indicate that there is a need for County Governments in Kenya to prepare for cybersecurity related challenges through policy formulations, End-users and ICT experts awareness on cybersecurity-attacks, Management support through resources funding and cybersecurity infrastructure is key to any system controls. The solutions to cybersecurity vulnerabilities in Kenyan County governments can be solved when these keys are implemented.

**Corresponding author: E-mail: vkadima@mmust.ac.ke;*

Keywords: Cybersecurity; vulnerability; attacks; threats.

1. INTRODUCTION

Modern computer technologies and an Internet connection has fundamentally improved people's lives in the society, the advancements in technology have led to the increase in attacks to computer systems thus posing serious threats. A security research report by the Computer Security Institute has shown that 32% of organisations in the past had experienced serious attacks caused by malware as the main challenge [1]. Computer systems can be vulnerable if they are not secured by installing proper security measures, such as use of strong passwords, licensed and updated antivirus software's and firewalls, failure to update operating systems or security measures that are supposed to be implemented, such weaknesses in systems expose them to attacks [2]. A computer system breach may cause serious losses and risks to confidential data and may lead to system failure [3]. Cybersecurity being the subject of concern, in this paper emphasis is on cybersecurity vulnerability as the challenge affecting County Governments in Kenya. However, we know very well that cybersecurity is a National concern. This paper addressed the key departments in County Governments which include Salaries, Revenue, and ICT, administration, Procurement and Public service boards. The County Governments in Kenya have a similar structure thus the paper will discuss two County Governments in Kenya, namely Kakamega and Bungoma where research was conducted to represent the rest. The target population was limited to ICT experts and computer users. ICT systems within the County Governments formed part of the study area. This paper is structured into six sub-sections as described in the following paragraph. Sub-section one contains the introduction of the paper including the problem statement, introduction, related studies and objectives. Section two presents the methodology applied in this paper the section further discusses Design approaches used, target population, sampling techniques and sample size used and data collection instruments. Section three discusses a detailed analysis of results and the findings. In section four, the paper presents the conclusions.

1.1 Statement of the Problem

Cybersecurity is a key determinant on how information systems operate in County Government's service delivery. Vulnerabilities could lead to attacks which jeopardise the normal functioning of systems. Attacks to Vulnerable systems will continue to be exploited as the County Governments adapt to changing technological advancements. An analysis of existing models, frameworks, systems and strategies to control these attacks indicates that most organisations have the initiatives but lack the zeal to implement on drafted measures which need to be highlighted and implemented. There are no workable initiatives on the key facilitating factors of cybersecurity in county governments and therefore may not be applicable to County Governments and cannot control the cybersecurity attacks adequately. The study was based on Kenyan County Governments due to increase in cyber-attacks, a report by [3] indicated that Kenyan organisations had lost US$ 20 Million through cyber-crimes, this figure has since increased where Kenya has lost US$ 206 Million through cybersecurity [4]. Most of this attacks have taken place through existing systems which are too vulnerable like for the case of IFMIS which lacks basic security procedures has been registering various malfunctions leading to loss of funds in county governments and other national ministries [5]. Hence the need for research to determine the key facilitators of cyber-crime in County Governments.

1.2 Objective

The objective of this paper is to determine the key facilitators of cybersecurity vulnerabilities in County Governments in Kenya.

2. RELATED WORK

Cybersecurity's related work in this paper will discuss matters related to cyber-attacks and how the various firms have managed them. County government just like any other organisations are at risk of various attacks which can pose as insider attacks to systems since data can be affected by network attacks directly or indirectly. In this paper, security is a key concern only the vulnerability element of security will be discussed [6]. A vulnerability can be explained as a technical flaw or weakness in the design, implementation, or operation and management that can be exploited to violate any system's security [7]. Vulnerabilities are a key threat to users and the systems they operate, the threats

become serious risks which can be exploited by network attacks the measures put in place to counter this attack is what will control them [8]. Cyber security has become a threat and has caused many challenges to organisations due to the costly risks they incur, in most cases some of the security strategies used have not been able to control the attacks, few organisations have used measures such as ensuring that computer systems are connected with computer security provisions by the affected organisations, unfortunately, this measures have not worked due to the new upcoming cyber-attacks [9].

In order to understand the concept of cybersecurity in detail, the paper sort further definitions of the term cybersecurity, According to [10], [11] and Cyber security is the act of protecting ICT systems and their contents. In this paper, cyber security can be defined with reference to previous authors who included [2] and ([9], they all define cybersecurity to include the key areas of concern which includes information technology security, focuses on protecting computers, networks, programs and data from unintended or unauthorized access, change or destruction. In this context, such security measures like use of firewalls, antivirus software, use of technical tools to secure computer data and networks are important and quite reliable in ensuring total security for the entire system [12]. Previous studies indicate that measures of controlling cyber-attacks were initiated through determinations on what tasks are key to the user's role, responsibilities, and requirements and can assist in assessing the user's behaviour, performance and proficiency skills such initiatives did not yield any controls as required by the experts [13]. Some of the hindrances from previous studies include uncertainties in defining the unknown user's role within the cybersecurity environment as basic control procedures and the ways of providing technical support, poor infrastructure, organizational behaviour on preparedness and training of users.

Key challenges experienced by the Kenyan government where numerous cybersecurity attacks had been exhibited on their systems, the attacks were targeting sections, such as accounts and organisations websites. The affected departments included Kenya Defence Forces whose social accounts were attacked. Further attacks were at the Deputy Presidents office and the ministry of foreign affairs sections websites. The hackers were responsible for numerous activities and most of this attacks were discovered to be anonymous [14]. The attackers who could latter on be referred to as cyber-terrorists managed to take advantage of the vulnerabilities in a major system used by the government known as Integrated Financial Management Information System (IFMIS), all the national and county government financial transactions are managed through this systems which were seriously affected and most departments lost funds due to the attacks. Further analysis as indicated in this paper is that hacking of computer systems, just like terrorism and piracy, is a major threat that is a global concern and should be taken seriously in order to reduce the increased attacks due to the vulnerabilities in our systems [15].

Any serious government both national and county that embraces modern technology should be able to plan well to control cybersecurity threats that could affect the nation. Through security initiatives done by the government, security related reports were drafted [13]. The county governments did not show any better initiatives on cybersecurity, hence they are supposed to have early plans on the countries initiatives to control cyber-insecurity due to the critical state caused by cyber-attacks in Kenya. Cyber-attacks have increased by 108% nationally. This is because of serious gaps in critical cybersecurity infrastructure, hence most systems that are vulnerable have been a quick target by attacks. Well exhibited cases in this paper that affected cases could include the use of electronic banking, website portals that require credit transactions, are not well protected and do not have proper ways of protection hence it's easy for attackers to access the clients information. Various banks are the most affected since previous research show that the majority of them did not secure their systems and just a few had managed to protect them through data encryption. Because of the inadequacies in security mechanisms of our banking systems, most of them are highly exposed to attacks, hence an easy target by cyber-criminals [16].

The national government has put in place strategies to manage cybersecurity matters through policies [17]. Drafted laws like the Kenya Information and Communications Act CAP 411 (2012), its main role is to offer a legislative guide to the government on matters information. One key challenge with the law is that it's not able to

solve all the possible cybersecurity related crimes but for initiative purposes, it can be used in managing and controlling the vulnerabilities. Further amendments to Information and Communications Technology law have been done to include offences to include unauthorised access to computers leading to modification of files this is an issue that has been cited in many cases that are affecting organisation today. Another challenge with this law was that since its enactment, the Kenyan government has not implemented the law to ensure that cyber related offenses are prosecuted [18]. There are various cases of cyber-related offences that have affected many organisations, this has become a serious concern by concerned agencies since the laws have not been able to prosecute cyber-criminals locally due to the weaknesses in the entire prosecution procedures in the country. Because of these inequalities, it has been noted that the main reason is the government does not have a proper mechanism to investigate and prosecute cyber related offences. In addition to the weaknesses in the prosecution procedures, most offences are complex because of the advancements in technology thus serious offenders have not been able to be prosecuted because of the weaknesses in the investigation processes [13]. Studies on cybersecurity should focus on measures to implement cyber related legislations and improve on technologies to be used in cyber-crime related offences. In order to seriously manage the risks caused by cybersecurity nationally, most of the cyber related laws should be implemented and new ones drafted. The new cyber-crimes bill enacted in 2018 will enable the county governments to leverage on and control cybersecurity crimes.

3. METHODOLOGY

In order to achieve its objective the paper used exploratory design where both qualitative and quantitative research approaches were adopted in the study [19]. Exploratory research design is the collection of information in an unstructured and informal manner often used when little is known about a problem. Creswell [20], defines mixed methods research as an approach to an inquiry involving collecting both quantitative and qualitative data, integrating the two forms of data, and using distinct designs that may involve philosophical assumptions and models.

The paper addresses a new phenomenon of study in Kenya where after the enactment of the new constitution, the Kenyan government formulated County Governments which are responsible of managing key functions that were dealt initially by the national governments. The national government devolved part of its services to county governments this brought about adoption of ICT in most of their functions thus security becoming a serious concern.in this paper, only two counties of Kakamega and Bungoma have represented the rest in Kenya .All County Governments in Kenya have a minimum of 15 Sub-Counties in this case 30 of them were under study. Kenya as a Country it has a total of 47 County Governments. This focus was done so because of the same structure and key functions they operate at that level. Most County Government's use the Integrated Financial Management Information Systems (IFMIS) has the following modules which are key, payroll e-procurement and human resource. The entire ICT infrastructure and internet communications this formed the basis for sources of cyber-attacks [21].

In order to calculate the sample size used, it was necessary to know the population size too. Population is defined as all elements that meet the sample criteria for inclusion in the study [22]. The paper used a target population of 170 employees as respondents all drawn from Bungoma and Kakamega County Governments. Out of 170 respondent 40 were ICT experts while 130 were End-users. The two Counties were chosen to represent County Governments in Kenya.

Sample size was obtained using the Yamane's method formula as shown below [23].

$$n = \frac{N}{1 + N(e^2)}$$

Using this formulae ***n*** is the desired sample size of the study population, ***N*** is the total study population, ***e*** is the level of statistical significance level.

$$n = \frac{40}{1 + 40(0.05^2)} = 37$$

Strata sample sizes are determined by the following equation

$$n_h = \frac{N_h}{N} \times n$$

Where

$$n_h = \frac{N_h}{N} \times n$$

$$n_h = samle\ \ size\ \ for\ \ strata$$

$$N = the\ \ total\ \ population\ \ size$$

$$n = the\ \ total\ \ sample\ \ size$$

$$N_h = population\ \ size\ \ for\ \ strata$$

$$n_h = \frac{30}{40} \times 37 = 27 \text{ (ICT Department)}$$

The sample size for each strata was determined using proportionate stratification approach. With proportionate stratification, the sample size of each stratum is proportionate to the population size of the stratum. The paper used interview schedules and questionnaires as data collection instruments. Two sets of questionnaires were administered to the sample, where one set was administered to the End-users and the other set to the ICT Experts all from different departments, each item in the questionnaire was developed to address the objective. Interview guides were used to collect information from the heads of ICT sections.

In order to check for reliability and validity, questionnaires administered to a section of respondents the questions were based on information gathered during the interview and literature review to ensure that there was representative of what respondents know about cybersecurity. Before the actual study, the instruments were discussed with supervisors. For validity purposes the paper used a valid measure of 0.5 which is acceptable as spearman correlation coefficient.

The study involved use of human respondents, hence ethical issues were considered.

In order to consider ethical issues for respondents, the respondents were educated on their rights in the study. Oral and written Consent was obtained and documented from all the study subjects prior to the interview. The respondents were assured of their participation which was voluntary and that the information was handled in a confidential manner, their names were not be used in any publication or presentation. The participants were asked of their free will to take part in the research without forcing or coercing them after being informed on the purpose of the inquiry. The option to withdraw from the research was also be explained to them. The researcher obtained an approval from the Board of Postgraduate students of Masinde Muliro University of Science and Technology, and an approved permit from NACOSTI. The researcher presented a letter from the university to the research site to seek authority to carry out the research and obtained permission from the County Government.

3.1 Data Analysis Methods

According to Denscombe [24], Data analysis involves the search for things that lie behind the surface content of the data – core elements that explain what the thing is and how it works. The analysis of data was done using thematic analysis where interview schedules and observation were used as sources of data. Data analytical tools were used to run descriptive statistics to produce frequency distribution, and percentages [14]. Descriptive statistics is concerned with organizing and summarizing data at hand, to render it more comprehensive while inferential statistics deals with the kinds of inferences that can be made when generalizing from data, as from sample data to the entire population [25]. The descriptive statistics that were used included measure of central tendency, mean, mode and median, standard deviation and variance [14].

4. PRESENTATION AND DISCUSSION OF RESULTS

This section provides the results and related discussions.

4.1 Demographic Distribution of Data

This section represents demographic distribution of data. Data is distributed across various demographic factors like gender, age bracket, and level of education, work station, and name of County as indicated in Table 1.

From the Table 1 a total of 37 IT Experts questionnaires were distributed, 25 in Kakamega County and 12 in Bungoma County. This shows that 55(65.1%) in Kakamega County were more represented as compared to 43(43.9%) from Bungoma County.

Table 1. Distribution of end users respondents by County Government

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Bungoma	43	43.9	43.9	43.9
	Kakamega	55	56.1	56.1	100.0
	Total	98	100.0	100.0	

Source: Research Data

Table 2. Distribution of ICT experts respondents by County

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Bungoma	12	32.4	32.4	32.4
	Kakamega	25	67.6	67.6	100.0
	Total	37	100.0	100.0	

Source: Research Data

Table 3. Demographic distribution of end users by County

		Frequency	Percent	Valid Percent	Cumulative Percent
Name of county	Bungoma	43	43.9	43.9	43.9
	Kakamega	55	56.1	56.1	100.0
	Total	98	100.0	100.0	
Gender	Male	54	55.1	55.1	55.1
	Female	44	44.9	44.9	100.0
	Total	98	100.0	100.0	
Age	18-24	32	32.7	32.7	32.7
	25-29	18	18.4	18.4	51.0
	30-35	28	28.6	28.6	79.6
	36-44	12	12.2	12.2	91.8
	45 and above	8	8.2	8.2	100.0
	Total	98	100.0	100.0	
Education	Certificates	83	84.7	84.7	84.7
	Diploma	10	10.2	10.2	94.9
	Degree	5	5.1	5.1	100.0
	Total	98	100.0	100.0	
Department	Finance	41	41.8	41.8	41.8
	County Assembly	24	24.5	24.5	66.3
	Procurement	19	19.4	19.4	85.7
	Secretariat	14	14.3	14.3	100.0
	Total	98	100.0	100.0	

Source: Research Data

4.2 Distribution of ICT Experts Respondents by County

The researcher sought to know the representation of ICT experts in the study. 12(32.4%) represented Bungoma County this was a lower representation compared to Kakamega County where 25(67.6%) were represented. This indicates that there are more ICT experts in Kakamega County as Compared to Bungoma County.

4.3 Distributions of End Users in Both Counties

The paper in this section shows the distribution of end-users in both counties. Table 3 shows the analysis on the same.

The analysis shows that there are more end users in Kakamega 55 (56%) than in Bungoma county 43(44%), this was also addressed by the IT managers whom we interviewed in both counties. It was also noted that Kakamega

county has the highest number of sub-counties compared to Bungoma county this explains why Kakamega county has the highest number of users. The analysis also shows that 54(55%) of the respondents are males while 44(45%) of the respondents are female. On the other hand the analysis shows that the majority of the end users 32(32.7%) are 18-24 years. The analysis also shows that majority of the users 83(84.7%) have certificate while 41(42%) work in finance department. Generally, it was found out that the majority of users are not ICT Experts since both counties have automated most of their functions which requires them to implement.

4.4 Factors influencing Cyber Security in County governments

The paper further discusses the key facilitating factors for cybersecurity in county government. Table 4 shows the analysis of how this factors influence cybersecurity attacks in county governments.

From Table 4 a Likert scale analysis was done and that 96(98%) of respondents agree that ICT infrastructure is an important factor that can influence cybersecurity for County Governments while on the other hand 89(90.9%) of the respondents agree that policies, regulations and legislation are important, for compliance and addressing challenges of cybersecurity attacks, county governments are required to draft policies and regulations that will guide in the implementations of this laws. The analysis also shows that 61(60.2%) of the respondents agree that resources and funding is important for cybersecurity while 71(72.5%) of the respondents agree that security of cybersecurity is important for the county government, there is need to input resources to manage cybersecurity infrastructure which is critical due to inadequate funding or no budgeting for the same. It is also noted from the analysis that 78(79.6%) of respondents agree that education awareness is important for cybersecurity while 77(78.6%) of respondents agree that staff experience is important for the cybersecurity for the county. The analysis also shows that 84(85.7%) of top management staff agree on the importance of addressing matters affecting cybersecurity with all the ICT staff in agreement on cybersecurity supported by 60(61.3%) of respondents who agree on the importance of preparedness for cybersecurity.

4.5 Funding of Cyber Security by County Governments

The researcher also sought to find out whether cybersecurity is funded by the county government. The analysis shows that 34 (91.8%) of the respondents agree that the county government is required to budget for cybersecurity related issues while 30 (81.1%) of the respondents agree that funding is one of the causes of vulnerabilities in county government. The analysis also shows that 29 (78.4%) of the respondents agree that adequate funding will control and reduce cybersecurity attacks in county government. On the other hand 33 (62.1%) of the respondents agree that the county government budgets are not adequate and does not include cybersecurity. Table 5 indicates the analysis of funding for county governments.

Table 4. Analysis on cybersecurity influencing factors in county governments

Cybersecurity Influencing Factors	Frequency									
	SD		D		N		A		SA	
	N	%	N	%	N	%	N	%	N	%
ICT Infrastructure	0	0	0	0	2	2	44	44.9	52	98
Policies & Regulations	0	0	0	0	9	9.2	37	37.8	52	89
Security	0	0	17	17.3	10	10.2	19	19.4	52	72
Resources and funding	0	0	16	16.3	21	21.4	10	10.2	51	60
Education Awareness	8	8.2	10	10.2	2	2	36	36.7	42	79
Staff Experience	0	0	10	10.2	11	11.2	15	15.3	62	78.6
Top Management Support	0	0	10	10.2	4	4.1	19	19.4	65	66.3
ICT Staff	0	0	0	0	0	0	31	31.6	67	85.7
Preparedness	11	11.2	8	8.2	19	19.4	18	18.4	42	61.3

Source: Research Data

Table 5. Analysis of cybersecurity funding by county governments

Funding	Frequency									
	SD		D		N		A		SA	
	N	%	N	%	N	%	N	%	N	%
Budgeting for cybersecurity related issues	3	8.1	0	0	0	0	17	45.9	17	45.9
Inadequate Funding is one of the causes of vulnerabilities	4	10.8	0	0	3	8.1	23	62.2	7	18.9
Adequate funding will control and reduce cyber-attacks in county governments	0	0	1	2.7	7	18.9	23	62.2	6	16.2
No budgets for cybersecurity	0	0	9	24.3	5	13.5	14	37.8	9	24.3

Source: Research Data (2018)

4.6 Adequacy of Cybersecurity Funding

The researcher sought to find out whether funding for cybersecurity is adequate in County Government. The analysis shows that 16(43.2%) of the respondents agree that cybersecurity matters are not budgeted while 23(62.1%) of the respondents agree that cybersecurity risks are too costly. The analysis also shows that 27(73%) of the respondents agree that funding is not adequate while 22(59.4%) of the respondents agree that cybersecurity experts are too expensive to hire and 24(64.8%) of the respondents agree that cybersecurity matters are too costly to implement.

4.7 Cybersecurity Policies and Regulations

The researcher also sought to find out whether there are cybersecurity policies and regulations in the county government. The analysis shows that 30(81.1%) of the respondents agree that the County Governments are required to formulate policies and regulations on cybersecurity related issues while all the respondents 37(100%) agree that County Governments are required to adopt and implement formulated policies and regulations on cybersecurity related issues and 34(89.2%) of the respondents agree that County Governments are required to revise/review adopted and implement formulated policies and regulations on cybersecurity related issues. On the other hand 30(81.1%) of the respondents are in agreement that County Governments are required to revise/review adopted and implement formulated reports on cybersecurity related issues while 23(62.1%) of the respondents are in agreement that there is no cybersecurity policies and regulations. The analysis also shows that 23(62.1%) agree that there is less initiatives to draft reports in cybersecurity matters while 17(45.9%) disagree that drafted reports and policies are not implemented and 14(41.5%) of the respondents agree that inadequate experts to lead initiatives of drafting policies on Cybersecurity matters while 19(51.3%) of the respondents agree that County Governments have not shown any plans/approaches to implement and formulate Cybersecurity legislations and policies.

4.8 Cybersecurity Technological Infrastructure

The researcher sought to find out on technological aspect of security and infrastructure in county governments. The analysis shows that 36(97.3%) of the respondents agree that the County Governments are required to install proper cybersecurity control measures while 31(83.7%) of the respondents agree that the County Governments need to adopt and implement improved cybersecurity infrastructure and 27(73%) of the respondents agree that County Governments cybersecurity matters is a concern and needs to be addressed. The analysis also shows that 34 (91.8%) of the respondents agree that the County Governments are experiencing new evolving cyber-attacks which needs to be controlled while all the respondents 37(100%) agree that the County Governments ICT Staff are required to install, update, modify passwords frequently to control cyber-attacks and 35(94.6%) of the respondents agree that the County Governments ICT Staff are required to install security measures to control insider-attacks. On the other hand 32(86.5%) of the respondents agree that the County Governments ICT Staff are required to identify attacks to systems and install necessary infrastructure to control cyber-attacks while 27(72.9%) of the respondents agree that County Governments are running critical cybersecurity infrastructure. The analysis also shows that 32(86.5%) of the respondents agree that there are inadequate cybersecurity experts to manage attacks while 27(73%) of the respondents agree that there are Challenges on security control measures by ICT Staff. From the

Table 6. Analysis of cybersecurity adequate funding by County Government

Funding for cybersecurity matters	Frequency									
	SD		D		N		A		SA	
	N	%	N	%	N	%	N	%	N	%
Cybersecurity matters are not budgeted	8	21.6	6	16.2	7	18.9	6	16.2	10	27.0
Cybersecurity risks are too costly	3	8.1	4	10.8	7	18.9	14	37.8	9	24.3
Funding is not adequate	5	13.5	3	8.1	2	5.4	21	56.8	6	16.2
Cybersecurity experts are too expensive to hire	8	21.6	7	18.9	0	0	11	29.7	11	29.7
Cybersecurity matters are too costly to implement	3	8.1	7	18.9	3	8.1	12	32.4	12	32.4

Source: Research Data (2018)

Table 7. Cybersecurity analysis on policies and regulations

Policies and Regulations	Frequency									
	SD		D		N		A		SA	
	N	%	N	%	N	%	N	%	N	%
Policy formulation	0	0	7	18.9	0	0	0	0	30	81.1
Adopt and implement Policies	0	0	0	0	0	0	9	24.3	28	75.7
Review of policies	0	0	0	0	4	10.8	6	16.2	27	73.0
Review formulated reports	0	0	3	8.1	4	10.8	11	29.7	19	51.4
No policies and regulations	0	0	6	16.2	8	21.6	16	43.2	7	18.9
Initiatives to draft reports	0	0	11	20.9	5	13.5	18	48.6	3	8.1
Drafted policies are not implemented	5	13.5	12	32.4	5	13.5	8	21.6	7	18.9
Inadequate experts	0	0	5	13.5	6	16.6	7	21.6	7	19.9
Plans to formulate legislations and policies	0	0	12	32.4	6	16.2	3	8.1	16	43.2

Source: Research Data (2018)

analysis, 32(86.5%) of the respondents agree that there are new advancements in technology while 31(83.8%) of the respondents agree that there are new and advanced cybercrime related activities. The researcher sought to find out if there was any significant difference in the mean of response from respondents in Kakamega County and Response from Bungoma County. The null hypothesis was tested at 5% significance level.

5. CONCLUSIONS

This paper, based on the study findings, established the following as key factors to enhance cybersecurity; the training of staff on cybersecurity awareness, hiring of cybersecurity experts, draft relevant policies and implementing them, review such laws when required, improving on critical cybersecurity infrastructure, adequate funding for cybersecurity, change with new advanced technologies related to cybersecurity and lastly the implementation of all this factors that influence cybersecurity attacks and implement all drafted cyber laws. Further, the paper suggests that this approach can be applied by any other organisations since most of the existing initiatives on cybersecurity have capacities which will be supported by this paper. The study would also contribute to cyber security research as it looks into deficiencies identified from the model analysis and provides improvement strategies against malicious insiders and outsiders. The insight would be useful to individuals employed in critical infrastructure areas as well as security agencies charged with protecting critical assets to assist them build or improve defenses against insider and outsider cyber threats. The information generated in the course of study would also enrich the body of knowledge on cybercrimes in the country and the Public Service. To future researchers and academicians, the study would be important in the suggestion of areas requiring

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

COMPETING INTERESTS

Authors have declared that no competing interests exist.

REFERENCES

1. Wang J. The deterrent and displacement effects of information security enforcement. International evidence. Journal Management Information System. 2010; 21(1):125-144.
2. ITU. Cyberwellness profile report. ITU, Kenya; 2014.
3. Wang P. The deterrent and displacement effects of information security enforcement. International evidence. J. Manag. Inf. Syst. 2010;125–144.
4. Serianu. Kenya Cyber Security Report 2018. Serianu Cyber Threat Intelligence Team (Serianu LTD), Kenya; 2018.
5. Okoth E. Daily Nation. 8 January; 2017. [Online].
   Available:http://www.nation.co.ke/news/State-audit-finds-serious-loopholes-in-Ifmis-system/1056-3509548-format-xhtml-7xl0jv/index.html.
   [Accessed 17 October 2018]
6. Blair D. Annual threat assessment: House permanent select committee on intelligence. House Permanent Select Committee on Intelligence, US; 2009.
7. Nandakumar N. Emerging and upcoming threats in cyber security in 21 century. International Journal of Computer Science and Mobile Computing (IJCSMC). 2007; 6(2):107-118.
8. Jingguo. An investigation of network attacks and vulnerability. ACM Transactionson Management, Information Systems; 2010.
9. Boyce. Human performance in cybersecurity. In Proceedings of the Human Factors and Ergonomics Society 55th Annual Meeting; 2011.
10. Fischer EA. Cybersecurity issues and challenges report. Congressional Research Service, CRS –Report prepared for members and committee of congress, US; 2016.
11. ISACA. State of cybersecurity: Implications for 2015 An ISACA and RSA Conference Survey. ISACA, USA; 2015.
12. Boyce M. Human performance in cybersecurity. In Proceedings of the Human Factors and Ergonomics Society 55th Annual Meeting, London; 2011.
13. Boyce. Human performance in cybersecurity. In Proceedings of the Human Factors and Ergonomics Society 55th Annual Meeting; 2011.
14. Chelanga M. Cyber-criminals hack Government of Kenya at will and the State is Helpless. Wednesday August; 2014. [Online].
   Available:http://ilaw.co.ke/tech-and-innovation/cyber-criminals-hack-government-of-kenya-at-will-and-the-state-is-helpless/#.WQiaesb-vIU
15. Muthengi M. Combating current and emerging cybercrimes in Kenya. International Journal of Education and Research. 2015;3(11):113-119.
16. Serianu. Cyber security strategy report. Government of Kenya, Nairobi; 2016.
17. Kenya GO. Computer misuse and cybercrimes act, 2018, Kenya. Imperial Journal of Interdisciplinary Research (IJIR). 2017;3(4):4.
18. Kiragu G. The relationship between executive compensation and risk among commercial banks in Kenya. Prime Journal of Social Science (PJSS). 2013;2(2):204-212.
19. Kothari C. Research Methodology Methods & Techniques, New Delhi: New Age International Publisher; 2004.
20. Creswell J. Research design: Qualitative, quantitative and mixed methods approaches (4th ed.). London: SAGE Publications, Inc.; 2017.
21. Chelanga M. Eastafrican Standard Newspaper. Wenesday August; 2014. [Online].
   Available:http://ilaw.co.ke/tech-and-innovation/cyber-criminals-hack-government-of-kenya-at-will-and-the-state-is-helpless/#.WQiaesb-vIU.
   [Accessed Monday October 2018].
22. Gathua & Kiragu, "The relationship between executive compensation and risk among commercial banks in," Prime

Journal of Social Science (PJSS), pp. 204-212, 2013.

23. Yamane T. Statistics: An Introductory Analysis. 3rd Edition, New York: Journal of Scientific Rresearch; 1973.
24. Denscombe M. The Good Research Guide Fourth Edition, New York: Unioversity Press; 2010.
25. Mouton. Understanding Social Research, Pretoria: Van Schaik; 1996.

Peer-review history:
The peer review history for this paper can be accessed here:
http://www.sciencedomain.org/review-history/27215