Cyber- Security Vulnerability and Initiatives in Kenyan County Governments

[1]Kadima Victor Chitechi [2]Benjamin Kiprono [3]Frank Tireito

[1,3]Masinde Muliro University of Science and Technology
Kakamega, Kenya
[2] Kaimosi Friends University, Kenya
vkadima@mmust.ac.ke ,benjaminkiprono@kafuco.ac.ke, ftireito@mmust.ac.ke

ABSTRACT

Globally, ICT is regarded as a driver and enabler thus; organisations, which have integrated ICT into their systems, have had immense growth and output. The adoption of ICT into the Kenya's County Governments therefore promises 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 sort to establish the current state of cyber security vulnerability, initiatives and factors affecting the state of cybersecurity in County Governments .The study was carried out in two counties namely Kakamega and Bungoma. The study targeted a total population of 170 staff grouped as end users and ICT Experts. The study adopted exploratory research design. Stratified random sampling technique was used to group the counties while purposive sampling was used to identify the correspondence with the required information. A sample size of 98 end users and 37 ICT experts was obtained using Yamane's formula. Questionnaires and interview schedules were used in data collection. The data was analyzed using SPSS where descriptive statistics of frequencies, charts, percentages and means regression analysis were used and a null hypothesis was tested at 5% level of significance. Study results showed that there is a positive association between preparedness and awareness hence a strong indication that the County Governments are not well prepared to manage cyber security matters in Kenya.

Keywords: Cybercrime, Cyber security, Vulnerabilities, computer crime, cyber threat.

1. Introduction

Modern computer technologies and Internet connection has fundamentally improved people's lives in the society, this advancements in technology has led to an increase in cyber-attacks on computer systems thus posing serious threats. A security research report by the Computer Security Institute has shown that 32% of organizations in the past had experienced attacks caused by malware (Mukunga, 2017). Computer systems can be vulnerable if 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 (Willis, 2013). A computer system breach may cause serious losses and risks to confidential data and may lead to system failure (PNG, 2010).

Some users in organisations can pose insider attacks to systems since data can be affected by network attacks directly or indirectly. 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. The vulnerabilities are a key threat to users since the threats become serious risks that can be exploited by network attacks (Jingguo, 2010).

Cyber security has become a threat and can pose many challenges to the users of information systems if the security measures are not taken care of. The challenges can be managed through use of security provisions to affected organisations. Some of these measures have not worked due to the new upcoming cyber-attacks. Cyber security can be defined as measures designed to protect a computer or a computer system against unauthorized access or attack (Boyce, 2011).

According to Suraj (2013) Cyber security is a process by which computer systems are secured through well-defined processes which includes various technological controls. In this context such security measure like use of firewalls, antivirus software, use of technical tools to secure computer data and networks is important and quite reliable in ensuring total security for the entire system (Atul, 2013). 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 behavior, performance and proficiency skills (Boyce, 2011). Some of the hindrances from previous studies include uncertainties in defining the unknown user's role within the cyber security environment and the ways of providing technical support and training of users.

Threats to cyber security can be broadly divided into two groups: actions aimed with intentions to crash cyber systems and efforts that seek to exploit the cyber infrastructure for unlawful or harmful purposes without damaging or compromising that infrastructure (Blair, 2009).

In certain circumstances some intrusions to systems may not necessarily be seen as a threat that can impact on the normal operation of a computer systems, a good example can be when a Trojan Horse penetrate and fixes itself in a computer, such intrusions are regarded as cyber-attacks when they can thereafter allow actions that damage the computer's functioning capacities.

Technical standards for the Internet are drafted and implemented by the privately controlled Internet Engineering Task Force (IETF) which is a Web Consortium, housed at the Massachusetts Institute of Technology, The main role of the consortium is to define technical standards for the Web (Clark, 2016). Other standards that have been used and are privately managed entities and play very key operational roles on aspects of cyber security includes, major telecommunications carriers, Internet Service Providers (ISPs), and some government organizations, including(Mukunga, 2018b). The Forum of Incident Response and Security Teams (FIRST) there has been attempts to coordinate the operations of both government and private Computer Emergency Response Teams (CERTs) which also works on cyber security standards. The Institute of Electrical and Electronics Engineers (IEEE), which develops technical standards through its Standards Association in conjunction with the U.S. National Institute of Standards and Technology (NIST) (Knave, 2009).

The Kenyan government has been experiencing numerous cyber security attacks on their systems. The attacks were targeting sections such as accounts and organisations websites. The affected departments includes; Kenya Defence Forces whose social accounts were attacked, further attacks were at the Deputy Presidents office and the ministry of foreign affairs sections websites (Mwiti, Kibaara, & Mageto, 2020). The hackers were responsible for numerous activities and most of these attacks were discovered to be anonymous (Chelanga, 2014).

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 financial transactions are managed through this systems which were seriously affected and most departments lost funds due to the attacks.

Hacking of computer systems, just like terrorism and piracy, is a major threat that is of global concern. Governments that embrace modern technology are able to plan well for control cyber security threats that could affect their nations. Through security initiatives done by the government, security related reports were drafted a good example is the Serianu report on cyber security (Serianu,2016). 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. The report shows that cyber-attacks have increased by 108% in both the government and enterprises. The report cited critical cyber security infrastructure and new technological advancements as too vulnerable for attacks.

The report further indicated that 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(Mukunga, 2018a). 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 (Serianu, 2016).

Several initiatives done by the national government have set the basis for information security controls. One of such initiative was the Kenya Information and Communications Act CAP 411 (GOK,2012), this report is a legislative guide and cannot be able to solve all the possible cyber security related crimes but for initiative purposes it can be used in managing and controlling the vulnerabilities. Studies on cyber security should focus on measures to implement cyber related legislations and improve on technologies to be used in cyber-crime related offenses(Serianu, 2016).

2. Statement of the Problem

The adoption of information systems operate in County Government's service delivery in Kenya has made cybersecurity to be key in entire process. Vulnerabilities can lead to attacks thereby jeopardising the normal functioning of any system. Attacks to vulnerable systems will continue to be exploited as the County Governments adapt to changing technological advancements can are a quick target as well as exposed to threats.

Most county governments are in the process of implementing new systems which require prior protection. There are little of no initiatives as they adopt to new systems due to the strategies laid out. County Governrnemts may not be ready manage serious cyber security attacks. Reports on cyber security by (Serianu, 2014) shows that Kenyan organisations lost Kshs 2billion through cyber-crimes in 2014, the figure has increased to 21.2 Billion as per the latest report by (Serianu, 2017). Cyber security incidences can be caused by not being able to initiate early preparations to control cyber-attacks. Furthermore, there are no workable initiatives to show how prepared the county government are. Hence, this paper draws a strong gap and basis for studying by determining the current state of cyber security vulnerability, initiatives and factors affecting the state of cybersecurity in County Governments in Kenya.

3. Objective of the study

This papers main objective is to determine the current state of cyber security vulnerability, initiatives and factors affecting the state of cybersecurity in County Governments in Kenya.

4. Related studies

Currently, initiatives on cyber security are still on and some developing countries have functional Computer Emergency Response Team (CERT) while others have additional protection measures apart from policies (Hale, 2017). Cyber-attacks are still prevalent. Most organisations are still experiencing numerous similar attack types that have afflicted organizations for decades. This has made it very difficult to source for skilled cyber security experts. The management support by the executives and board members are very concerned about new cyber-threats and how they are negatively impacting on organisations technologies and offer new technology-based services and products they have to ensure that the security of systems is well designed and that any information and data is protected.

4.1 Cyber Security Vulnerability Initiatives in Africa

According to Kristina_(2008), cyber-attacks has shown new trends. Majority of African countries are still at the initiative stage on security matters since few are in the process of drafting laws related to cyber security policies and regulations. Some nations have not started security initiatives but are concentrating on cyber-crime laws (Kamau & Chege, 2017). Developing nations have been creating cyber-crime legislation; these laws are essentially an effort on the part of government to protect national security by fighting potential cyber-terrorism. There is need for other factors being included to fully address cyber security apart from policies and regulations since this two cannot entirely manage cyber-attacks. Some gaps exist in that we expect factors such as new advancements in technology and cyber security infrastructure addressed. Cyber security laws and regulations in developed nations is key when handling the security of information .Most developing countries have the perception that cyber security challenges can only affect the national security, this has made most of them can be reluctant on protecting their information system hence unable to conform to improved security requirements for a given nation (P. Ndunge, Kamau, & Gikandi, 2016). Cyberattacks largely defy the simple categorization of activity defined by existing laws making it difficult for nations to apply the traditional definitions of crime, terrorism, warfare or espionage as understood under existing law. Traditional classifications of crime, terrorism, and warfare break down due to the aforementioned asymmetric nature of network communication. By giving non-state actors access to a new, diffuse kind of power, cyberspace erodes states' monopolization of the ability to wage war and effectively levels the playing field between all actors (Stahl, 2011).

The legal and legislative analyses of cybersecurity issues must distinguish among not only different cyber-threat categories enumerated above and actors, such as nation-states, terrorists, criminals, and malicious hackers, but also among different types of cyber-threats. Such cyber-threats include threats to critical infrastructure, which could lead to loss of life or significant damage to our economy; and threats to intellectual property, which could affect a nation's long-term competitiveness (Appazov, 2014).

4.2 Regional State of Cyber Security Vulnerabilities

The regional security of any nation's information systems is key and is a matter of concern to the various organisations. Currently, cyber security has been conventionalized to form East Africa, which comprises of Kenya, Uganda, Tanzania, Burundi, and Rwanda. The conventional or such union was formed in 2007 at a time when the member states were still in the initial stages of drafting laws (GOK, 2007). East African Community is a major driving force and an enabler in practicing key cyber security legislations within member groups this is done as part of the agreement on Electronic protections of data awareness. Similarly, other nations have laws to control cyber-crimes while some nations are still in the process of drafting the laws. Different countries have legislations inform of Acts that can be used to control how the users are managing the data and the computer itself, The Computer Misuse Act (2003) was published by Mauritia's to cover cyber-crimes like unauthorized access and interference in data transmission. (GOM, 2004). The Act instituted harsh punishment on cyber offenses, which included twenty-five years of imprisonment.

In Kenya, the first draft legislation known as the e-Transactions Bill was proposed in 2004. The bill was drafted in order to manage online transactions thereby attract the investors from outside the country and cyber security related challenges. The law was to be used as a basic model on all the electronic matters affecting the nations within that convention. (Reba, 2005). Some countries organised for cyber security awareness, for example, the Ethiopian ICT Development Agency however, this has not indicated if the initiative has affected the security (M. P. Ndunge & Kamau, 2017). There are special cases where a countries legislation on cyber-crime is still in the drafting process, such laws might not be implemented since the enactment has not been realized. The Ugandan law on internet communication was drafted to enable all internet service providers ensure there is proper protection on all the services they provide. Some laws might be difficult to interpret and implement if the terms used are not well understood by the users (ITU, 2005). This convention has been creating initiatives that geared on other key areas of concern for cyber security like training of users and awareness. We cannot rule out if some countries are still in the process of preparing to show signs of taking initiatives for cyber security (ITU, 2017).

4.3 Cyber security Vulnerabilities Preparedness in Kenya

Most nations have taken initiatives to control cyber security matters and critical infrastructure by involving top managers within organizations, Such efforts ensure that many different players from different organisations are engaged (Dunn, 2005).

According to World Summit Information Society Thematic Meeting report on Cyber security 2015, it was through such initiative that important sections were created and delocalized to manage security within the government structures. Key factors at some levels were managed individually for example a country like Austria created a unit to manage its main risk of critical infrastructure in the country thereby protecting it from outside attacks and to prevent all the information contained in computers. Security and infrastructure are just part of the factors required to manage cyber security matters other factors like funding, cyber security practitioners, awareness needs to be addressed (Dunn,2005).

According to (Okuku, 2015), developed nations have been using key initiatives in the protection and security of information systems and related laws for some time, reviews to security policy are done and adopted thereby implementing cyber security legislation. In preparedness to control cyber security matters some laws had to be drafted as an approach in reducing the cyber-attacks this laws include;

i) Data protection and security in electronic communications

ii) Management support to information and data protection through compliance like ISO/IEC 17799, ISO/IEC 15408.

To fully control the cyber-attacks it is important to entirely address the matter by not just focusing on security and policies, but to include other factors such as awareness, funding, and infrastructure and cyber security staff. Another gap in this literature is the strategy to implement the drafted laws or legislations on cyber security that has been cited as a key issue in this study (Sharma, 2007).

The County Governments in Kenya are still working on the initiatives of managing the cyber security vulnerabilities affecting the functions and operations of the counties. Cyber security regulations, laws, policies have been created to act as initiatives to curb cyber-attacks in Kenya. The national government is in the process of implementing most of the regulations that had been drafted and same regulations have adopted by the county governments since the counties have only been there for four years (Okuku, 2015). The main role of KE-CIRT/CC is cyber security matters , Communications Authority is mandated by the Kenyan laws of 1998 to establish a national cyber-security management framework this will ensure that Kenya Computer Incident Response Team Coordination Centre (KE-CIRT) is well coordinated and manage all security related incidents nationally (Nyange, 2015). KE-CIRT/CC is also has capacity to maintain awareness on information security activities (Okuku, 2015). As a country, more laws were drafted through Government agencies to manage cyber security challenges a good example of such agencies was the Kenya information and communications act (KICA) The Draft KICA Cyber security Regulations, (2016) aimed to regulate:

i) Operation and use of cyber cafes and public wireless hotspots
ii) Management of critical Internet resources
iii) Promotion of local content
iv)Localization of public information and dot KE domains
v) Data retention and protection requirements
vi)Framework for reporting, investigating
vii) Prosecuting and response to cyber
viii) Crime under the National KE-CIRT/CC and Jurisdictional provisions.

The Kenyan government in 2010 drafted the Kenya Information and Communications Regulations. The regulations have since been reviewed its mandate was regulation of Electronic Certification and Domain Name Administration. Also being drafted are regulations on Cyber security and E-Commerce (KLR, 2010).

According to the Kenya cyber security report (2015) there are user friendly approaches that can be used on certain key environments this includes, computer related hardware's, users , stakeholders and clients learning about cyber-attackers with the intention to attack such environment. Initiatives have been made and through several security regulations were drafted unfortunately there has been very little impact on cyber-attacks in Kenya. The approaches used to implement the same policies have been ineffective and there is need to improve on the way they should be implemented (Serianu,2015).

Some of the offenses made by known attackers are using various ways to execute their tasks this includes; unauthorised logins and stealing of password. It is prudent that organisations should learn to enact laws that will guide them in the training of staff on all security matters. The ability of an organisation to have security plans in place has an easy task when making key decisions on cybersecurity. In this report we can simply conclude that the majority of drafted cyber security frameworks are globally in design and therefore cannot be in a position to manage the organisations failed to address local situations where many small organisations have unique information risk requirements (Muchai, 2017). Localized Cyber intelligence and research is critical in understanding the type of attacks that might face counties in general. Many technology vendors will provide you with cyber intelligence which are global in nature and does not put into account any local intelligence. To be fully secure you need to develop local cyber intelligence capabilities that will enhance the visibility of the threats facing your organisations.

Most Kenyans believe that criminals are increasingly targeting organisations like the county government, reports have alluded that such organisations do not have enough staff and security expertise dedicated to cybersecurity. The majority of respondents say their organisations are increasingly becoming concerned and have partially implemented proper security precautions, technology and training. The security measures most often reported as being implemented by IT practitioners are perimeter systems like firewalls and anti-viruses (ISACA, 2015).

According to Serianu, Kenya cyber security report 2016 whose mandate was to ensure that there is Awareness and Training, Continuous Monitoring and Log Analysis, Vulnerability and Patch Management, Continuous Risk Assessment and Treatment, Services and Independent Reviews. The report explains that Technology has changed due to increased use of Optical Fiber Technology, introduction of 4G network capabilities and numerous companies are now offering Cloud computing services as more businesses digitize their business processes and move to the internet, hence exposure to cyber-attacks (Muthengi, 2015). This new operational environment requires unpatched software. In addition, the internal teams are unaware of these vulnerabilities. The report has addressed key factors in cyber security however the report does not show how the suggestions will be implemented. The funding for the highlighted issues will be sourced, this makes it difficult to implement. The new vulnerabilities need detailed studies to analyse and come up with the ways to manage them (Musuva, 2018).

Due to the lack of visibility among Kenyan organisations, they are making the wrong investments in security infrastructure and thus failing to store and transmit within networks. Sources of an attack can be an insider, a hacker or a terrorist, the consequences are often the same loss of revenue, sensitive information, erosion of consumer and constituent confidence and interruption or denial of business operations(Kimani,2016). One of the most critical challenges facing Kenyan organisations is the lack of awareness among technology users. Many of these users mostly customers and employees have little knowledge of the level of risk they are exposing themselves and their organisations to. These security lapses have exposed many Kenyan organisations to phishing and other social engineering related attacks. To manage this the Government of Kenya developed the Serianu Cyber Security report whose main role is to identify and prioritize specific risks and steps that can be taken to address cyber security risks in a cost effective manner (Kimani, 2016). The report is limited on how complicated and advanced cyber-attacks can be managed. The issue of cyber security practitioner's inadequacy has not been captured in the report and it's one of the key issues affecting cyber security today.

5. Methodology

Random sampling technique was used where a target population of 170 employees were used as respondents all drawn from Bungoma and Kakamega County Governments. The target population of the ICT experts was obtained from the records of employees in the two Counties. The end users were chosen randomly from the employees using the ICT interfaces within the County department. Out of 170 respondent 40 were ICT experts while 130 were End-users.

5.1 Sample Size

Sample size was obtained using the Yamane's method formula as shown below (Yamane, 1973).

$$n = \frac{N}{1 + N(e^2)} \qquad (3.1)$$

From Equation (3.1), ***n*** represents the desired sample size of the study population, ***N*** is the total study population, while ***e*** is the level of statistical significance level n (error term).

$$n = \frac{40}{1 + 40(0.05^2)} = 37 \qquad (3.2)$$

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. Strata sample sizes are determined by the following equation

$$n_h = \frac{N_h}{N} \times n \qquad (3.3)$$

Where

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

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

$N = the\ total\ population\ size$

$n = the\ total\ sample\ size$

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

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

Table 3.1: Sample Size for ICT Expert Respondents

Department	Target population	Sample population
IT	30	27
Other Ministries	6	6
Revenue	2	2
Salaries	2	2
Total	40	37

Source: Researcher (2018)

Sample size for End-users was obtained using the Yamane's method formula as shown Equation (3.1).

The sample size for each strata was determined using proportionate stratification approach shown in equation (3.3). With proportionate stratification, the sample size of each stratum is proportionate to the population size of the stratum. Strata sample sizes are determined by the following equation

$$n_h = \frac{24}{130} \times 98 = 18 \text{ (End-users IT)}$$

Table 3.2: Expected Sample size for End-Users respondents

Department	Target population	Sample population
IT	20	19
Other Ministries	60	52
Revenue	20	19
Salaries	8	8
Total	**108**	**98**

Source: Researcher (2018)

5.2 Reliability and Validity Tests

Reliability of an instrument being the consistency of an instrument in measuring what it is intended to measure was established by first ensuring internal constancy approach followed by carrying out a pilot study. A questionnaire is considered reliable if the Cronbach's Alpha coefficient is greater than 0.70 (Katou, 2008). The four independent variables and the dependent variable were subjected to reliability test using SPSS and the results obtained are shown in Table 4.1.

Table 4.1 Reliability test

Variable	Cronbach alpha
Cybersecurity vulnerability	.923
Preparedness and awareness	.986

Support and funding	.883
Policies and regulations	.817
Technology	.883

Source: (Researcher, 2018)

The results indicated that all the variables obtained had Cronbach's Alpha greater than 0.7 thereby achieving the recommended 0.7 for internal consistence of data (Mugenda & Mugenda, 2008).

Data validity is the degree to which a test measures that which it is supposed to measure (Porter, 2010). Mugenda and Mugenda (2008) define validity as the degree to which the research results obtained from the analysis of the data represent the phenomenon under study. According to Table 4.2 Kaiser–Meyer-Olkin measure of sampling adequately indicated KMO value of greater than 0.5 meaning thereby that the sample size was good enough to treat the sampling data as normally distributed. Bartlett's test sphericity which tested the null hypothesis "item to item correlation matrix based on the responses received from respondents for all the effective variables was an identity matrix". The Bartlett's test was evaluated through chi-square test having as shown in Table 4.2 for the entire variables and were all significant at 0.000 level of significant, indicating that null hypothesis is rejected.

Table 4.2 Test for validity

Factors	KMO test	Barlett's test of sphericity		
		Chi-Square	df	Sig.
Cybersecurity vulnerability	0.871	221.45	4	0.000
Preparedness and awareness	0.958	176.65	4	0.000
Support and funding	0.932	167.34	4	0.000
Policies and regulations	0.929	188.72	4	0.000
Technology	0.873	190.18	4	0.000

Extraction Method: Principal Component Analysis.
Source: (Researcher, 2018)

5.3 Demographic Characteristics of the Respondents

This section contains the analysis of information on respondent's age, gender, education level work station, and name of County. The main purpose of this was to find out any trend from the respondents profile that was directly linked to the variables of the study.

Table 4.1 Distribution of End Users Respondents by County

County	Frequency	Percent	Valid Percent	Cumulative Percent
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 (2018)

There were 98 questionnaires fully filled and returned from Kakamega and Bungoma Counties. A total of 37 IT Experts questionnaires were distributed, 25 in Kakamega County and 12 in Bungoma County. All the questionnaires issued were returned

Table 4.2 Distribution of ICT Experts Respondents by County

	Frequency	Percent	Valid Percent	Cumulative Percent
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 (2018)

5.4 Demographic distribution of End Users by County

Table 4.3 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 (2018)

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

6. Study findings

The main objective of this paper was to establish the current state of cyber security vulnerability in County Governments in Kenya. In order to achieve the above objective, this paper sought to find out how cybersecurity preparedness and awareness in County Governments. Table 4.4 below represents the quantitative analysis of the state of cybersecurity vulnerability. 5 Scale Likert scale was used and the results are as shown;

Table 4.4 Quantitative analysis of the state of cyber security

State of Cybersecurity	Frequency									
	SD		D		N		A		SA	
	N	%	N	%	N	%	N	%	N	%
Awareness on cybersecurity-attacks	0	0	0	0	0	0	5	23.5	32	86.5
Occasional trainings for users and ICT experts on cyber-attacks	0	0	0	0	0	0	9	24.3	28	75.7
Prepare and address cybersecurity matters in time.	0	0	0	0	0	0	14	37.8	23	62.2
Initiatives in controlling and sharing new-trends on cybersecurity issues	0	0	0	0	0	0	11	29.7	26	70.3
Adoption of proper control measures in preparedness to manage cyber-security matters	0	0	2	5.4	0	0	10	27	25	67.6
Manage cyber-attacks through trainings	0	0	3	8.1	1	2.7	11	29.7	22	59.5

Source: Research Data (2018)

From the analysis of the Likert scale, majority of the ICT experts 32 (86.5%) strongly agree that all users and ICT experts are supposed to be made aware of cybersecurity-attacks in county governments while on the other hand 28 (75.5%) of the ICT experts strongly agree that there is need to train All users and ICT experts on cyber-attacks that County Governments are supposed to be Prepaired in addressing the cybersecurity matters in time while 26 (70.3%) of the ICT experts strongly agree that County Governments are supposed to make initiatives with other organisations in controlling and sharing new-trends on cybersecurity issues. It is also noted from the analysis that 25 (67.6%) of ICT experts strongly agree that ICT experts are supposed to adopt on proper control measures in preparedness to manage cyber-security matters in county governments and 22 (59.5%) of the ICT expert strongly agree that the training of staff on cybersecurity matters will enable the control and spread of cyber-attacks in County Government. The findings above thus indicate that both county governments are still in the process of establishing the initiatives to address cybersecurity matters. Hence, both county governments are not prepared to address cybersecurity matters.

Table 4.5. Analysis of the Likert Scale on ICT Experts Preparedness on Cybersecurity

Cybersecurity Preparedness	**Frequency**									
	SD		**D**		**N**		**A**		**SA**	
	N	**%**	**N**	**%**	**N**	**%**	**N**	**%**	**N**	**%**
Drafting of policies	0	0	8	8.2	12	12.2	57	58.2	21	21.4
Training	0	11	2	11.2	2	2.0	53	54.1	32	32.7
Hiring of experts	8	8.2	15	15.3	21	21.4	21	21.4	33	33.7
Funding	8	8.2	10	10.2	2	2	47	48	31	31.6
Security measures	0	0	0	0	2	2	52	52	44	44.9

Source: Research Data (2018)

The analysis shows that 57(58.2%) of the end users agree on drafting of cybersecurity regulations/laws while 53(54%) of the end users agree that training and awareness on cybersecurity matters is important. On the other hand 33(33.7%) of end users strongly agree on employment of cybersecurity experts. The analysis also shows that 47(48%) of end users agree that cybersecurity should be funded while 52(52%) of end users agree on security measures to control cybersecurity. From the above analysis, County Governments are still in the process of initiating plans for cybersecurity regulations/laws. There is need to employ cybersecurity experts in the county governments to manage the increasing cybersecurity challenges.

In this paper, the researcher further sought to find out whether inadequate preparation and training influenced cybersecurity attacks in County Governments, the researcher did the analysis and the study findings are as shown in table 4.9 below.

Table 4.9 Cybersecurity Analysis on Preparedness and Awareness (type of analysis xxxxxx)

	Frequency									
	SD		D		N		A		SA	
Preparedness and Awareness	N	%	N	%	N	%	N	%	N	%
Inadequate experts	3	8.1	0	0	6	16.2	18	48.6	10	27
Unpreparedness	0	0	3	8.1	8	21.6	18	48.6	8	21.6
Risks experienced	0	0	0	0	6	16.2	18	48.6	13	35.1

Source: Research Data(2018)

The analysis shows that 28(75.6%) of the respondents agree that most ICT staff are not well trained on matters to do with cybersecurity while 26(70.2%) of the respondents agree that the county government is not prepared to address cybersecurity matters. The analysis also shows that 31(83.7%) of the respondents agree that County Governments experiences risks caused by cybersecurity. This analysis indicate that county governments are not well prepared to manage cybersecurity challenges due to inadequate cybersecurity awareness and are exposed to more advanced risks caused by this factors.

7. Conclusion

The study sought to determine the current state of cyber security vulnerability, initiatives and factors affecting the state of cybersecurity in County Governments in Kenya. Through findings, this paper can strongly allude that the county governments are not adequately prepared to manage cybersecurity matters. This is because of the following. Inadequate funding, lack of cybersecurity preparation strategy or initiatives, new technologies, and critical infrastructure. The study recommendations based on the study findings that the following measures to be used an implementation strategy for preparedness and initiative; the training of staff on cybersecurity awareness, hiring of cybersecurity experts, draft relevant policies and implement them review such laws when required, improve critical cybersecurity infrastructure, adequate funding for cybersecurity, change with new advanced technologies related to cybersecurity.

8. References

Akinwake, A. T., & Ibharalu, F. T. (2009). Password Authentication Scheme with Secured Login Interface. *Annals Computer Science Seried* , pp. 77-85.

Alexander & Keith. (2006). Information Systems Security Education. *10th Annual Colloquium for Information Systems Security Education*.

Antoniou. (2012, November 02). Retrieved December 11, 2015, from http://www.isa.edu.gr/app/webroot/isafckfile/file/__HOMEWORK/ANTONIOU/10/Ch_11_Computer_security_and_safetyethics_and_privacy.pdf

Appazov, A. (2014). *Legal Aspects of Cybersecurity.* Copenhagen: University of Copenhagen.

Atul, S. a. (2013, may). Cyber security: challenges for society- literature review. *IOSR Journal of Computer Engineering (IOSR-JCE)*, pp. 67-75.

Blair, A. D. (2009). Annual Threat Assessment. *House Permanent Select Committee on Intelligence,* .

Boyce. (2011). Human Performance in Cybersecurity. *Proceedings of the Human Factors and Ergonomics Society 55th Annual Meeting.*

Boyce. (2011). Human Performance in Cybersecurity. *Proceedings of the Human Factors and Ergonomics Society 55th Annual Meeting.*

Cetinkaya, O. (2008). *World Summit on the Information Society Stocktaking.* Geneva: International Telecommunication Union (ITU).

Chang, B. a. (2010).

Chelanga, M. (2014, August Wednesday). *Cyber-criminals Hack Government of Kenya At Will and the State is Helpless.* Retrieved from Eastafrican Standard: http://ilaw.co.ke/tech-and-innovation/cyber-criminals-hack-government-of-kenya-at-will-and-the-state-is-helpless/#.WQiaesb-vIU

Clark, A. &. (2016, june 07). Proceedings of a Workshop on Deterring Cyber Attacks. *Cyber Security and International Agreements ,Internet Corporation for Assigned Names and Numbers*, pp. 185-205.

Cole. (2008). Cybersecurity in Africa: An Assessment. *ITU.*

Conklin & Gregory. (2007). e-Government and Cyber Security , The Role of Cyber Security Exercises. *Proceedings of the 39th Annual Hawaii International Conference on System Sciences* (pp. 4-7). Kauai, Hawaii.: International Conference on System Sciences.

Craig, S. S. (2014). Analysing The Evolving Role of National Governments In Internet Governance and Enhancing Cybersecurity. *Stanford Journal of International Law.*

D., S. a. (2012). Proceedings of a Workshop on Deterring Cyber Attack. *Informing Strategies and Developing Options for U.S. Policy* (pp. 185-205). Cyber Security and International Agreements ,.

DHS. (2011). Enabling distributed security in cyberspace. *uilding a healthy and resilient cyber ecosystem with automated collective action.*

Dunn. (2005). A Comparative Analysis of Cybersecurity Initiatives Worldwide. *WSIS Thematic Meeting on Cybersecurity* (p. 5). Geneva: Swiss Federal Institute of Technology.

Edwin, O. (2017, January 8). *Daily Nation.* Retrieved from State audit finds serious loopholes in Ifmis system: http://www.nation.co.ke/news/State-audit-finds-serious-loopholes-in-Ifmis-system/1056-3509548-format-xhtml-7xl0jv/index.html

Gainey, S. (2016). *The Current State of Cyber Security for Financial Services.* Washington D.C: Great Western Bancorp, Inc.

GAO. (2014). *Cybersecurity for Critical Infrastructure Protection.* Google Scholar.

Gathua and Kiragu. (2013). The relationship between executive compensation and risk among commercial banks in Kenya. *Prime Journal of Social Science (PJSS)*, 204-212.

Gathua, K. a. (2013). The relationship between executive compensation and risk among commercial banks in Kenya. *Prime Journal of Social Science (PJSS)*, 204-212.

GOK. (2007). *E-legislation initiative for East African Nations.* Washington D.C: GOK.

GOK. (2014). *National cyber security strategy.* NAIROBI.

GOM. (2004). *The ICT sector in Mauritius: an overview.* Mauritius: GOM.

Hale, R. (2017, February 17). *Are We Winning the Cyber War? A Look at the State of Cybersecurity in 2016.* Retrieved from ISACA: https://www.isaca.org/Knowledge-Center/Blog/Lists/Posts/Post.aspx?ID=593

Hudson. (2001). Aviation safety culture. *Keynote address at Safeskies Conference*.

ISACA. (2015). State of Cybersecurity. *Implications for 2015 An ISACA and RSA Conference Survey* (pp. 2-5). USA: ISACA LTD.

ITU . (2016). Enabling Environment for the Greater Growth of the Internet. *World Conference on International Telecommunications 20.* Dubai: ITU.

ITU. (2017, February 18). *West Africa Workshop on Policy and Regulatory Frameworks for Cybersecurity and CIIP 27-29 November.* Retrieved from African Information Security Association: http://www.jidaw.com/security/aisa/aisa.html

Jingguo. (2010). An Investigation of Network Attacks and Vulnerability. *ACM Transactionson Management, Information Systems*.

Joseph, K. (2011). *Factor Affecting Effective Implimentation of Intergrated Management System (IFMIS).* Nairobi: UON.

Joseph, T. (2014). *National cyber security strategy* . Nairobi: ICT Authority.

Kaibunga, S. (2014). *Kenya Cyber Security Strategy.* Nairobi: Government of Kenya.

Kariuki, G. (2009). Growth and Improvement of Information Communication Technology in Kenya. *International Journal of Education and Development using ICT*, 1814-0556.

Kimani, K. (2016). *Kenya Cyber Security Report 2016.* Nairobi: Serianu Cyber Threat Intelligence Team.

KLR. (2010). *The Kenya Information & Communicatfions ACT 2010.* Nairobi: Government of Kenya.

Knave, C. (2009). Cyber security effectively negating further use. *IEEE*, 20 - 24.

Kohlbacher, F. (2006). The use of qualitative content analysis in case study research. *Qualitative social research* , 21.

Laban & Otuya. (2017). Integrated Financial Information System (IFMIS) and National and County Government Performance in Kenya-A Critical Analysis. *International Journal of Multidisciplinary and Current Research*, 2321-3124.

McConnell, M. (2014). How to Win the Cyber-war We're Losing. *acm* .

MDI. (2017, February 18). *Current State of CyberSecurity and Why More Companies Should Care.* Retrieved from IT Workforce Solutions: http://www.mdigroup.com/the-current-state-of-cybersecurity-and-why-more-companies-should-care/

Mohamed, G. a. (2015). Cyber Security and the Internet of Things:Vulnerabilities, Threats, Intruders. *International Journal of Cyber Security, Vol. 4, 65–88.*, 65-88.

Mouton. (2009). *Understanding Social Research.* Pretoria: Van Schaik.

Muchai, C. (2017). *Kenya Cyber Security Report.* Nairobi: Serianu Ltd.

Murithi & Mwinzi. (2016). he Influence of Financial Resources on the integration of the National Goals of Education. *International Journal of Education and Research*.

Musuva, P. (2018). *Kenya Cyber Security Report.* Nairobi: Serianu Ltd.

Muthengi. (2015). Combating Current and Emerging Cybercrimes in Kenya. *International Journal of Education and Research*, 113-119.

Ngundi, V. (2016). *Overview Of Kenya's Cybersecurity Framework.* Nairobi: GOK.

Nyange, H. (2015). Kenya‟s National Cyber Security Framework. *1Kenya"s Presentation to CAFRAD Conference of ICTSecurity and DefenceExperts* (pp. 23-25). Moroco: GOK.

Okoth. (2017, January 8). *State Audit finds Serious Loopholes in IFMIS* . Retrieved from Sunday Nations Report on Intergrated Financial Management System (IFMIS): http://www.nation.co.ke/news/State-audit-finds-serious-loopholes-in-Ifmis-system/1056-3509548-format-xhtml-7xl0jv/index.html

Okoth, E. (2018, January 8th). *State Audit finds serious loopholes in Intergrated Finance Management Information System (IFMIS).* Retrieved from Daily Nations Report onIntergrated Finance Management Information System (IFMIS): http://www.nation.co.ke/news/State-audit-finds-serious-loopholes-in-Ifmis-system/1056-3509548-format-xhtml-7xl0jv/index.html

Okuku. (2015). Cybersecurity Strategy's Role . *Information & Security: An International Journal.*

Paris, R. (2001). Paradigm Shift of Hot Air? International Security.

Parker & Hudson. (2006). A framework for understanding the development of organisational safety culture. *Safety Science*, 551–562.

PNG, W. a. (2010). The deterrent and displacement effects of information security enforcement. *International Evidence. Journal of Managing Information System*, 125–144.

Reba, B. (2005). *State of Cybersecurity.* ADIS ABABA: GOE.

Robert & YIN. (2009). *Case study Rresearch design and methods.* London: Sage Publication.

Serianu. (2016). *Cyber Security Strategy Report.* Nairobi: Government of Kenya.

Serianu. (2016). *Kenya Cyber Security Strategy.* Nairobi: Government of Kenya.

Sharma, S. (2007). *Teaching information systems security courses: A hands-on approach.* Indiana: Elsevier Journal Ltd. .

Stahl, W. M. (2011). The Uncharted Waters of Cyberspace: Applying the Principles of International Maritime Law to the Problem of Cybersecurity. *40 GEORGIA JOURNAL OF INTERNATIONAL AND COMPARATIVE LAW*, 247-274.

Tiampati, J. (2014). *National cybersecurity strategy Report.* Nairobi: ICT Authority.

Tonge, A. &. (2013). Cyber Security: Challenges for Society- Literature Review. *IOSR Journal of Computer Engineering (IOSR-JCE)*, 67-75.

WSIS. (2015). World Summit on the Information Society. *WSIS Forum 2013.* Dubai: ITU.