International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2020): 7.803

Cyber-Security Vulnerability Assessment Model for County Governments in Kenya

Kadima Victor Chitechi[1], Kelvin K. Omieno[2], Samuel Mbugua[3]

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

[2]Kaimosi Friend University College

[3]Kibabii University
Vkadima[at]mmust.ac.ke, komieno[at]kafuco.ac.ke, smbugua[at]kibu.ac.ke

Abstract: ***Computerization of county government daily activities enables faster and better services to their clients. The integration of Information and Communications Technology by the CG into their systems has led to new advancements in technology. The adoption of ICT into the Kenya's County Governments has contributed to faster growth and output in better client service delivery. The benefits has also encouraged serious attacks to such systems causing risks due to easier penetration in the systems because of vulnerabilities. The attacks have costed county governments more resources and time in case of managing such risks. As a country, we need to ensure that all our systems are well safeguarded from attacks. This paper sought to address the above issue bydeveloping a cyber-security vulnerability assessment model for County Governments in Kenya, The model can be applied as a better approach that will manage and reduce the attacks and risks. The Model was developed from a study that targeted a total population of 170 staff grouped as end users and ICT Experts working in county governments of Kakamega and Bungoma. The study adopted an 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 mean 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, support and funding, policies and regulations, and technology; hence influencing cyber-security. The developed model will be used as a guide to manage cyber security matters in Kenya's County governments.***

Keywords: Cyber-Security, Cyber-Attacks, Vulnerability, Assessment Model, Model, County Governments

1. Introduction

Currently, most organizations are experiencing technological advancements due to faster and reliable Internet connections. The high demand and full access to internet services has affected and improved peoples' lives (Nepal et al., 2014). Conversely, such accessibility if not well secured is prone to open in-security on systems. technological growth has led to an increase in cyber-attacks on computer systems thereby posing serious threats to various systems(Nepal, 2014).Computer threats to cyber-security are usually classified as attempts aimed with intentions to crash cyber-systems and efforts that seek to exploit the cyber-infrastructure for unlawful or harmful purposes with intention to damage or compromise the infrastructure (Blair, 2009).

Cyber-security is important and will indicate the growth and better daily functions to any country. Vulnerabilities to any systems can expose the entire information leading to serious attacks hindering the normal functioning of the organisation including the county governments. Numerous Attacks to weak points in any new system will easily be exploited especially the County Governments since they are in the process of adapting to changing technological advancements if proper control measures are not put in place. Recent cyber-security reports by (Serianu, 2018) show that most organisations are losing money due to cyber-attacks, existing cyber-security models have not been able to control this attacks. studies indicate that Kenyan organisations will have lost close to Kshs 22 billion through cyber-crimes by the year 2020(Paula Kigen, 2014), the figure might increase if strict measures are not followed. This indicates how the state of cyber-security in county government requires other manageable solutions. This paper will address such challenges by providing a lasting solution through a developed cyber-security assessment model that can address all the key factors affecting the County Governments.

The objective of the study was todevelop a cyber-security vulnerability assessment model for County Governments in Kenya

2. Research Methodology

In this paper, exploratory design was employed with both qualitative and quantitative research approaches being adopted. The core assumption of using this design was that the combination of qualitative and quantitative approaches provides a more complete understanding of a research problem than using only one methodology in the study (Cresswell J. , 2014).

2.1 Study Area

The study was conducted at Kakamega and Bungoma County Governments in Kenya. The research study focused on the County Governments in Kenya due to the structure and key functions they operate at that level. The entire ICT infrastructure and internet communications formed the basis

for sources of cyber-attacks that were discussed in the study. For uniformity of the study characteristics, Bungoma and Kakamega County governments were chosen to represent County Governments in Kenya

2.2 Study Target Population

Simple random sampling technique was used to determine the target population of 170 employees as respondents all drawn from Bungoma and Kakamega County Governments. A 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 within the County department. Out of 170 respondents, 40 were ICT experts while 130 were end-users.

2.3 Sampling and Sample Size

The study used purposive sampling to come up with the departments that were used to provide key informants for the study (Green, 2015). The key informants were selected using random sampling. Sample size was obtained using the Yamane's method formula as shown below (Yamane, 1973).

$$n = \frac{N}{1 + N(e^2)} \quad \text{..... (1.0)}$$

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 (error term).

$$n = \frac{40}{1 + 40(0.05^2)} = 37 \quad \text{..... (1.1)}$$

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

$$n_h = \frac{N_h}{N} \times n \quad \text{..... (1.2)}$$

Where

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

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

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

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

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

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

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

Table 1: Sample Size for ICT Expert Respondents

	Department	Target population	Sample population
ICT Experts	ICT	30	27
	Others	6	6
	Revenue	2	2
	Salaries	2	2
End-Users	ICT	20	19
	Ministries	60	52
	Revenue	20	19
	Salaries	8	8

Source: Kadima (2018)

2.4 Data Collection and Analysis

The study employed the use of pretested self-administered questionnaires and structured questionnaires. Finally, Interview guides were used in the study to solicit for information from the heads of ICT sections. Data analysis was done through the use of descriptive (measure of central tendency, mean, mode and median, standard deviation and variance) and inferential analysis (Kappa test and regression analysis).

2.5 Ethical Issues

Oral and written Consent were 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 (Saunders, 2009).

3. Related Studies

Cyber-attacks become more attractive and potentially more disastrous as our dependence on information technology increases. According to the Symantec cybercrime report published in April 2018, cyber-attacks costed US$114 billion each year (Julian Jang-Jaccard, 2018). If the time lost by companies trying to recover from cyber-attacks is counted, the total cost of cyber-attacks would reach staggering US$385 billion in the near future (Julian et al., 2018). Victims of cyber-attacks are also significantly growing due to technology advancements. Based on the survey conducted by Symantec which involved interviewing 20,000 people across 24 countries, 69% reported being the victim of a cyber-attack in their lifetime.

Due to emerging technologies, cyber-attacks on systems evolve through time capitalizing on new approaches. Most times, cyber criminals would modify the existing malware signatures to exploit the flaws exist in the new technologies. Cybersecurity is a term that can be used interchangeably with the term information security. There is a substantial overlap between the two terms, these two concepts are not totally analogous. Moreover, the paper posits that cyber security goes beyond the boundaries of traditional information security to include not only the protection of information resources, but also that of other assets, including the users (Rossouwvon Solms & Johanvan Niekerk, 2013). In information security, reference to the human factor usually relates to the role(s) of humans in the security process (Rossouwvon et al ,. 2013)

Security refers to a process to protect an object against physical damage, unauthorized access, theft, or loss, by

maintaining high confidentiality and integrity of information about the object and making information about that object available whenever needed in the paper objects refer to the systems being adopted by various organisations (Mohamed Abomhara & Geir M. Køien, 2015).

According to Mohamed (2015), Vulnerabilities are weaknesses in an organisations systems such as the county government or a poor system design that allow intruders to penetrate thereby execute commands, access unauthorized data, and/or conduct denial-of service attacks. The vulnerabilities can be weaknesses in system hardware or software, weaknesses in policies and procedures used in the systems and weaknesses of the system users themselves (Mohamed et al , . 2015).

Some of the attacks to organisations systems are caused by the users themselves due to not following the laid out policies. Insider-attacks have consistently been identified as key potential threats to organizations and governments (Neetesh Saxena, 2020). It is important to understand the nature of insider-attacks and the related threat landscape can help in forming mitigation strategies (Neetesh Saxena, 2020).

Computer systems if exposed can be very vulnerable especially if not secured through proper security techniques such as use of strong passwords,(Wang, 2010), installation of security tools such as licensed and updated antivirus software's or applications and firewalls is also another secure approach. The only risks if such security initiatives are not taken care of like failure to update operating systems or security measures that are supposed to be implemented may lead to weaknesses in computer systems thus exposing them to attacks(Jean-Paul A. Yaacoub, 2020). Such measures can only be put into practice when we have working models and implemented key security policies (Wang, 2010). This paper sought to develop cyber-security assessment model that can address the vulnerabilities in County Governments information systems.

4. Results and Findings

In order to find the factors that determine cyber-security vulnerability, a regression analysis was done where data was tested at 5% level of significance as shown in the table 2.0 below.

Table 2: Regression Analysis Model

Model	Unstandardized Coefficients		Standardized Coefficients	t	Sig.
	B	Std. Error	Beta		
(Constant)	2.828	0.942		7.184	0
Preparedness and Awareness	0.003	0.179	0.03	4.628	0.003
Support & Funding	0.361	0.054	0.342	6.714	0.001
Policies and Regulations	0.029	0.053	0.434	8.154	0.004
Technology	0.438	0.05	0.438	8.75	0
a. Dependent Variable: Cyber-security Vulnerability					

Research Data (2019)

The result shows that at 5% level of significance cyber-security vulnerability factors do not affect cyber-security. From the findings in Table 2.0; at 5% level of significance, preparedness and awareness is significant predictor of Cyber-security vulnerability where (p=0.03 < 0.05).

Letting Y be Cyber-security and vulnerability, X_1 be Preparedness and Awareness, X_2 be Support & Funding, X_3 Policies and Regulations, X_4 be technology, and ε is the error term. Using the regression coefficients in Table 5.1, we have

$$Y = \beta_0 + \beta_1 X_1 + \beta_2 X_2 + \beta_3 X_3 + \beta_4 X_4 + \varepsilon$$

$$Y = 2.824 + 0.003 * X_1 + 0.361 * X_2 + 0.209 * X_3 + 0.438 * X_4 + 0.942$$

From the equation above when preparedness and awareness is increased by one unit cyber-security vulnerability will increase by 0.003, a unit increase in support and finding will result to 0.361 increase in Cyber-security vulnerability, a unit increase in policies and regulation will result to 0.029 increase in Cyber-security and vulnerability, and lastly a unit increase technology will result to 0.438 increase in Cyber-security and vulnerability. Therefore the study model is;

*Cyber-security vulnerability = 21.134 + 0.003*preparedness and awareness + 0.361*support and funding + 0.029*policies and regulation + 0.438*technology + 0.942*

It is clear from the study model that Cyber-security vulnerability is greatly affected by support and funding, policies and regulations and technology this are the main factors.

The findings of the regression analysis led to the development of the model as shown in figure 1.0.

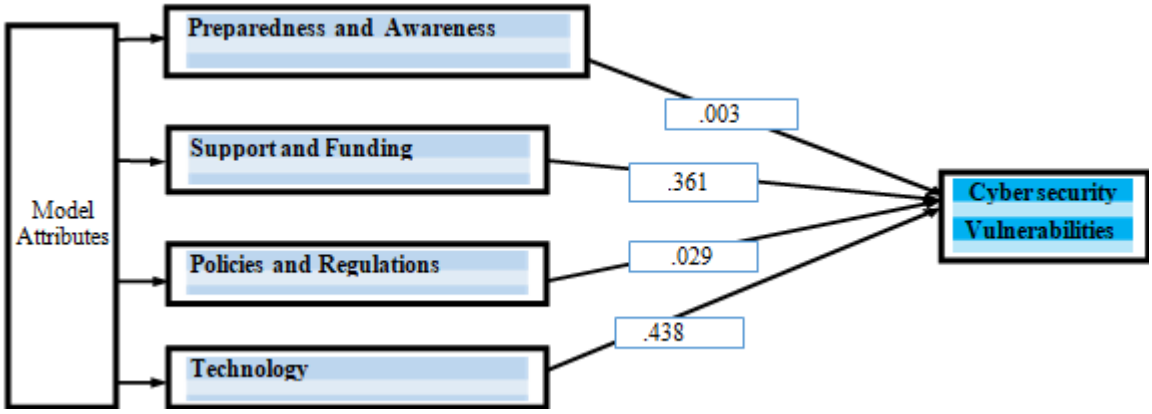

Figure 1: Cyber-Security Vulnerability Assessment Model (CSVAM)
Source: Kadima (2018)

4.1 Validation of Cyber-Security Vulnerability Assessment Model (CSVAM)

In this study, validation was done to check if the developed model could assess Cyber-security vulnerability in County Governments in Kenya (Pressman, 2004). The study-adopted use of expert analysis where 25 experts were invited on a focused group discussion where they were asked to analyse the model and give their opinions on what extend they perceived the model will be implemented to reduce Cyber-security attacks. Use of questionnaires was employed where sets of questionnaires and the developed model were distributed to the experts via electronic mail and their opinions analysed and discussed (Benini, 2017). The validations results were analysed and summarized in this section as shown below.

Table 2: Model validation statements

Factors	SA	D	N	A	SA
The model establishes the state of Cyber-security	0	2(8%)	0	3(12%)	20(80%)
The model determines the facilitators of Cyber-security attacks	0	4(16%)	0	0	21(84%)
The model addresses the level Cyber-security preparedness	0	0	0	6(24%)	19(76%)
The model addresses the key Cyber-security influencing factors	0	2(8%)	1(4%)	4(16%)	18(72%)
The model addresses key Cyber-security attacks	0	4(16%)	0	3(12%)	18(72%)
The model addresses Cyber-security policies and regulations	0	0	2(8%)	6(24%)	17(68%)
The model addresses Cyber-security support and funding	4(16%)	5(20%)	3(12%)	13(52%)	0
The model addresses Cyber-security infrastructure	3(12%)	9(36%)	0	13(52%)	0

Source: Kadima (2019)

The results indicates that 23(92%) of the respondents strongly agree that the developed model establishes the state of Cyber-security while 21(84%) of the respondents strongly agree that the developed model determines the facilitators of Cyber-security attacks. The analysis also shows that 25(100%) of the respondents agree that the developed model addresses the level Cyber-security preparedness and awareness while 22(88%) of the respondents agree that the developed model addresses the key Cyber-security influencing factors. On the other hand 23(92%) of the respondents agree that the developed model addresses Cyber-security related policies and regulations.

The analysis further showed that 21(88%) of the respondents agreed that the developed model addressed key Cyber-security attacks. From the analysis, 23(92%) of the respondents agreed that the developed model addresses Cyber-security policies and regulations. On the other hand 13(52%) of the respondents agreed that the developed model addresses Cyber-security support and funding while 9(46%) disagree. The analysis indicated that 13(52%) of the respondents agree that the developed model addresses Cyber-security support and funding while 12(48%) of the respondents disagreed.

The researcher sought to find out if there was any relationship in respondents from Kakamega County and Bungoma County. The researcher also sought to find out the level of agreement between the respondents of Bungoma County and Kakamega County. The Chi-square test was used to test for the association and Kappa test was used to test for the level of agreement. Using null hypothesis the study showed that there is no association tested at 5% level of significance.

Table 3: Kappa test Analysis of the two County Governments

Kappa Test Analysis Statements		Name of the county				Pearson χ^2 value	Kappa test
		Kakamega		Bungoma			
		N	%	N	%		
The model establish the state of Cyber-security	Disagree	1	7	1	9	0.916	0.859
	Agree	2	14	1	9		
	Strongly agree	11	79	9	82		
Total		14	100	11	100		

The model determines the facilitators of Cyber-security attacks	Disagree	2	14	2	18	0.792	0.792
	Strongly agree	12	86	9	82		
Total		14	100	11	100		
The model addresses the level Cyber-security preparedness	Agree	4	29	2	18	0.546	0.565
	Strongly agree	10	71	9	82		
Total		14	100	11	100		
The model addresses the key Cyber-security influencing factors	Disagree	1	7	1	9	0.831	0.859
	Neutral	1	7	0	0		
	Agree	2	14	2	18		
	Strongly agree	10	72	8	73		
Total		14	100	11	100		
The model addresses key Cyber-security attacks	Disagree	2	14	2	18	0.906	0.792
	Agree	2	14	1	9		
	Strongly agree	10	72	8	73		
Total		14	100	11	100		
The model addresses Cyber-security policies and regulations	Neutral	1	7	1	9	0.831	0.722
	Agree	4	29	2	18		
	Strongly agree	9	64	8	73		
Total		14	100	11	100		
The model addresses Cyber-security support and funding	Strongly Disagree	2	14	2	18	0.968	0.767
	Disagree	3	22	2	18		
	Neutral	2	14	1	9		
	Agree	7	50	6	55		
Total		14	100	11	100		
The model addresses Cyber-security infrastructure	Strongly Disagree	2	14	1	9	0.921	0.823
	Disagree	5	36	4	36		
	Agree	7	50	6	55		
Total		14	100	11	100		

Source: Kadima (2019)

At 5%, the level of significance the analysis showed that there was relationship between the response given by the respondents between the two Counties of Kakamega and Bungoma. This is because all the chi-square value are greater than 0.05 i.e. p> 0.05. This is confirmed by the Kappa test value which indicates highest level of agreement with values greater than 0.7. Hence, an indication that the model developed is valid and can be applied. The researcher further argues that the study achieved its main mandate.

5. Conclusion

Technology as a factor had more influence to Cyber-security vulnerability than preparedness and awareness i.e. the more the advance in technology the more Cyber-security vulnerability. The results in the model validation section show that the model will manage, control, reduce vulnerability and improve assessment of Cyber-security vulnerabilities in County Governments in Kenya.

6. Future Research

The study recommend the design of appropriate metrics and development of a tool out of the models.

References

[1] Atul M. Tonge1, S. S. (2013). Cyber security:challenges for society-literature review. *IOSR Journal of Computer Engineering (IOSR-JCE)e-ISSN: 2278-0661, p-ISSN: 2278-8727Volume 12, Issue 2(May. -Jun. 2013), PP 67-75 www.iosrjournals.orgwww.iosrjournals.org 2278-0661, p-ISSN: 2278-8727Volume 12, Issue 2(May. -Jun. 2*, 67-75.

[2] Benini, A. P. (2017, August). The Use of Expert Judgment in Humanitarian Analysis Theory, Methods,Applications. *Geneva, Assessment Capacities Project - ACAPS*.

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

[4] Boyce, M. (2015). Human Performance in Cybersecurity. *Proceedings of the Human Factors and Ergonomics Society 55th Annual Meeting* (pp. 1002-1006). Las Vegas, Nevada USA.: HFES-Human Factors and Ergonomics Society.

[5] 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

[6] 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.

[7] Cresswell, J. (2014). Research Design Qualitative, Quantitative and Mixed Methods Approaches 4th Edition. In C. J.W, *Research Design.* Canada: Canadian Center of Science and Education.

[8] Cresswell, J. W. (2016). *Planning , Conducting and Evaluating Qualitative and Quantitative Research.* London: Pearson Education Inc.

[9] Green, L. A. (2015). Purposeful Sampling for Qualitative Data Collection and Analysis in Mixed Method Implementation Research. *Administration and Policy in Mental Health and Mental Health Services Research, September 2015, Volume 42, Issue 5, pp 533–544*, 533-544.

[10] Ilker Etikan, S. A. (2016). Comparison of Convenience Sampling and Purposive Sampling. *American Journal of Theoretical and Applied Statistics,Published online December 22, 2015 (http://www.sciencepublishinggroup.com/j/ajtas) doi: 10.11648/j.ajtas.20160501.11*, 1-4.

[11] Jean-Paul A. Yaacoub, a. O. (2020). Cyber-physical systems security: Limitations, issues and future trends. *Elsevier Public Health Emergency Collection-Published online 2020 Jul 8. doi: 10.1016/j.micpro.2020.103201*.

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

[13] Julian Jang-Jaccard, S. N. (2018). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences-Volume 80, Issue 5, August 2014, Pages 973-993-https://doi.org/10.1016/j.jcss.2014.02.005*, 973-993.

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

[15] Kothari, C. (2010). *Research Methodology: Methods and Techniques.* Mumbai: New Age International publishers. .

[16] Michael Boyce, &. K. (2015). Human Performance in Cybersecurity. *Proceedings of the Human Factors and Ergonomics Society 55th Annual Meeting* (pp. 1002-1006). Las Vegas, Nevada USA: HFES-Human Factors and Ergonomics Society.

[17] Mohamed Abomhara & Geir M. Køien. (2015). Cyber Security and the Internet ofThings:Vulnerabilities,Threats, Intruders and Attacks. *Journal of Cyber Security, Vol. 4, 65–88-doi: 10.13052/jcsm2245-1439.414* , 65-88.

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

[19] Murithi Tiberious, M. J. (2016). The Influence of Financial Resources on the integration of the National Goals of Education . *International Journal of Education and ResearchVol. 4 No. 9 September2016*.

[20] Neetesh Saxena, E. H. (2020). Impact and Key Challenges of Insider Threats on Organizations and Critical Businesses. *MDPI Electronics Open Acess Journal* .

[21] Nepal, J. J. (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences,Volume 80, Issue 5, August 2014, Pages 973-993*, 973-993.

[22] Paula Kigen, C. K. (2014). *KENYA CYBER SECURITY REPORT 2014 Rethinking Cyber Security –An Integrated Approach: Processes, Intelligence and Monitoring.* Nairobi: Serianu Limited.

[23] Pressman, R. S. (2004). *Software Engineering: A Practitioner's Approach: 6th (Sixth) Edition.* ISA: McGraw-Hill Companies, The (March 24, 2004).

[24] RegDennick, M. T. (2011). Making sense of Cronbach's alpha. *International Journal of Medical Education. 2011; 2:53-55 , ISSN: 2042-6372 DOI: 10.5116/ijme.4dfb.8dfd*, 53-55 .

[25] Rossouwvon Solms & Johanvan Niekerk. (2013). From information security to cyber security. *Volume 38, October 2013, Pages 97-102 - https://doi.org/10.1016/j.cose.2013.04.004*, 97-102.

[26] Saunders, M. (2009). *Ethics in Research.* London: Pearson Education.

[27] Suraj, A. &. (2013, may). Cyber security: challenges for society- literature review. *IOSR Journal of Computer Engineering (IOSR-JCE)*, pp. 67-75.

[28] Thomas W. Edgar, D. O. (2017). Science and Cyber Security in Research Methods for Cyber Securit. In D. O. Thomas W. Edgar, *Research Methods for Cyber Security* (pp. 393-404). Elsevier B.V. .

[29] Wang, P. &. (2010). The deterrent and displacement effects of information security enforcement. *International evidence. J. Manag. Inf. Syst.*, 125–144.