ISSN No:-2456-2165

A Model for Assessing Information Security Preparedness Level in E-Governance in Kenya’s County Governments

Gladys Korir
Kabarak University

Abstract:- The purpose of the study is to discuss fundamental information security control measures that can be used to develop a model to determine organization information security preparedness level. The model utilizes a web-based platform containing specific information security indicators against which governments can assess their capability to protect e-governance systems. The study adopted design science research methodology to implement the model. The target population were selected based on their knowledge, experience and roles in e-governance. The study adopted cluster and simple random sampling methods. To evaluate the model, a goal-based approach was used. The study established that technological, environmental and organization controls measures directly contribute to organization information security and that their individual implementations level affects the security posture of an organization. The study provides a method by which governments can use to assess their information security control measures and hence work towards improving their organizational information security posture.

Keywords:- *E-Governance, Information Security, Information Security Control Measures, Organization Information Security Preparedness.*

I. INTRODUCTION

In an age where globalization and emerging technologies have taken root of every aspect of life, governments are now obligated to use new emerging and disruptive technologies to deliver public services. Governments are continually relying on information systems for efficient, accountable and transparent public service delivery (Nadu, 2013). E-governance is becoming a formal way of providing improved public services. The resultant benefits of e-governance are less corruption, increased transparency, greater convenience, revenue growth, and cost reductions (Wamoto, 2015). Countries globally are increasingly taking up on utilization of ICTs to deliver public services, increase transparency and engage people in decision-making processes. According to the United Nations E-Government Survey 2016, there has been an inclined rise in the number of countries utilizing advanced electronic and mobile services to provide public services online through one-stop platforms.

In Kenya, electronic governance has been supported momentously as an ideal remedy for improving governance and enabling other critical functions of the government (Ochara, 2008). In 2004, the Kenyan government approved the e-government plan marking the start of e-governance journey in Kenya (Wamoto, 2015). Since then, the government of Kenya has initiated several e-governance systems with the aim of enhancing efficiency, transparency and democracy within public administration. The implementation of these systems however, has encountered several challenges, which include technical challenges –like security and privacy of information, inadequate infrastructure, financial challenges due to inadequate funding, social issues and human challenges(Meiyanti et al., 2019).

Security and privacy of information is a major technical challenge facing e-governance initiatives in Kenya(Wamoto, 2015). Citizens’ concerns about their information and transactions privacy is one of the major factors influencing the success of e-government initiatives. Information security is a critical element in the implementation of any e-governance initiative(Shareef, 2016). Information security ensures that the confidentiality, integrity and availability of information are protected. In Kenya, information security in e-governance have been addressed using different approaches but still appear to be weak. For instance, the government of Kenya was reported to have lost over $171million to cyber-crimes by the end of 2017, which is said to be the highest record in East Africa (Cisco, 2017). Today’s governments and organizations employ very sophisticated security tools and technologies like firewalls, encryption, access control management, and others to curb this challenge. While advanced security technologies are fundamental parts of operational information security practices, it has been observed that appropriate security technologies alone are not adequate in addressing information security challenges (Otero, 2014).

In order to enhance information security, governments and organizations need to evaluate their information security practices on a regular basis so as to determine their security capability and thus review and update their information security practices to satisfy their specific security requirements and to overcome the challenge of the dynamic nature of information security threats (Otero, 2014).Enhancing information security in e-governance not only nurture secure e-governance services, but also, builds confidence and trust in e-governance system users(Masau et al., 2011); leading to the success of e-governance initiatives (Karokola, 2012)

- *Problem Statement*

According to Cisco cyber security annual report 2017, in East Africa Kenya recorded the highest loss of $171 million to cyber criminals by the end of 2017. The public sector was ranked as the sector facing the highest information and cyber security risks in Kenya. This is so, not because the government has not invested in ensuring information security, but because of lack of realistic and prioritized strategies for improving organizational information security measures (Cisco, 2017). Due to the dynamic nature of information threats and emerging technologies, government should invest in techniques for regular assessment of information security control measures in order to establish the ability of the existing strategies in protecting information. This fact, therefore, necessitates the need for developing more efficient and innovative ways of evaluating organization's information security control measures. Departments responsible for critical government infrastructure need to have a consistent and iterative way of identifying, assessing and managing organization's information security. Adequate evaluation of information security control measures employed in governments is crucial in sustaining sound security as well as protecting information assets. Present information security assessment methodologies like risk assessment and management, best practice frameworks and other ad hoc approaches need to be reinforced and improved to assist governments with the process of information security management.

- *Objective*

The purpose of this paper is to discuss the fundamental information security control measures that can be used in assessment of organization information security preparedness level

II. LITERATURE REVIEW

- *Information Security Assessment*

Information security assessment is the process of determining how effectively an entity being assessed (such as host, system, network, procedure, and person) meets specific security objectives(Scarfone & Orebaugh, 2008). Information security assessment practices vary between industries, disciplines, and even within the same organization, which has brought about many different approaches of assessing information security in an organization. There are three broad categories of assessment methods that can be used to assess information security measures; testing, examination, and interviewing. Testing is the process of analyzing one or more assessment objects under specified conditions to compare actual and expected behaviors. Examination is the process of checking, inspecting, reviewing, observing, studying, or analyzing one or more assessment objects to facilitate understanding, achieve clarification, or obtain evidence. Interviewing is the process of conducting discussions with individuals or groups within an organization to facilitate understanding, achieve clarification, or identify the location of evidence. Assessment results are used to support the determination of security control effectiveness over time.

There are different existing methodologies for information security assessment developed by different organizations and researchers to assist organizations assess their information security preparedness. There is no precise methodology that has been developed to address information security assessment problem in Kenya. Although there are numerous information security assessment methodologies available, none of them is a fit for all solution.

To perform an assessment on information security preparedness level of an organization, one must identify key information security controls employed by the organization to secure their information systems. Information security controls are technical or administrative safeguards and counter measures employed to avoid, counteract or minimize loss or unavailability of information due to threats acting on their corresponding vulnerability(Keung, 2014). Information security controls seek to protect the confidentiality, integrity, availability and assurance of information. Information security control measures are core components of organization information security management system. They are administered to prevent, detect and correct information security risk through administrative, technical and physical means.

National institute of Standards and Technology (NIST) lists the three primary categories of controls as administrative, technical and physical (Keung, 2014). Administrative controls are primarily, procedures and policies which are created to define and guide employee actions in dealing with the organizations' sensitive information. Technical security controls consist of those hardware and software features provided in a system that helps to ensure the integrity and security of data, programs and operating systems. Physical security controls are means and devices employed to control physical access to sensitive information and to protect the availability of the information(Eduardo & Junior, 2015).

Security controls can be further classified based on the phase of activities involved in implementing them and the purposes for which they are implemented. Information security controls can be grouped as preventive controls or detective controls or corrective controls depending on the objective of implementation. Preventive controls are implemented to prevent the threat from coming in contact with the weakness. Detective controls are controls that identify that the threat has landed in systems. Corrective controls are controls that mitigate or lessen the effects of the threat being manifested.

III. METHODOLOGY

The study was carried out in Uasin Gishu county government. The research target population included the county executive members, ICT staff, chief information security officers in the counties and information systems users and custodians within the county governments. Respondents were selected based on their knowledge, experience and roles in e-governance and information security.

The study adopted cluster and simple random sampling methods. Each of the five categories of respondents with knowledge and experience in e-governance that constitute total population were considered as a cluster for the study. Simple random sampling method was used to identify respondents in each cluster. The total population targeted by the study was 40 people. The study used structured questionnaire as the primary data collection instrument.

Analysis of the findings was done using descriptive statistics and inferential statistics in the form of frequency distributions, percentages measures of central tendencies and positions, regression and correlation analysis to establish any emerging patterns which were presented in tables. Pearson correlation was used to test the nature of relationship among the variables. The model was tested by using a goal-based evaluation approach which determines the extent at which the model was achieving its predefined objectives.

IV. DATA ANALYSIS AND PRESENTATION

The study distributed 40 questionnaires and all were filled and collected. This gave a response rate of 100%.

- *General Background Information*

Characteristic	Frequency	Percent
Chief Information security officers	2	5.0
County executive members	3	7.5
ICT staff	10	25.0
Information system custodians	10	25.0
Information system users	15	37.5
Total	40	100.0

Table 1:- Job Title

Descriptive analysis such as percentages was used to examine distributional patterns of variables under study. The independent variables were descriptively analyzed and the findings presented in subsequent tables. The chi-square (χ^2) values indicated is the chi-square goodness of fit which shows how data was distributed across the distributional categories. The p-values also indicated the relationship between the observed values and the expected values of the different variables analyzed, however does not indicate the significance of the variable analyzed. P-values less than 0.05 shows that there was a significant difference between the observed values and expected values while that greater than 0.05 shows that there was no significant difference between the observed values and expected values.

- *Information security preparedness Indicators*

The dependent variable was analyzed in terms of the following indicators.

Statement	X1	X2	X3	X4	X5	χ^2	p
Access controls	0.0%	50.0%	32.5%	17.5%	0.0%	6.35	0.042
Server and network security	15.0%	35.0%	0.0%	32.5%	17.5%	5.00	0.172
System software security	0.0%	17.5%	50.0%	32.5%	0.0%	6.35	0.042
Data security	0.0%	47.5%	17.5%	35.0%	0.0%	5.45	0.066
Human Resource Security	0.0%	15.0%	67.5%	17.5%	0.0%	21.05	0.000
Security awareness, training and education	15.0%	32.5%	17.5%	35.0%	0.0%	5.00	0.172
Information security policy	17.5%	17.5%	50.0%	15.0%	0.0%	13.40	0.004
Physical and environmental security	0.0%	17.5%	35.0%	30.0%	17.5%	3.80	0.284
Compliance	0.0%	32.5%	17.5%	35.0%	15.0%	5.00	0.172
Key: X1= Not implemented; X2= only some part has been implemented; X3= Implemented but has not been reviewed; X4= Implemented and reviewed on regular basis; X5= fully implemented and recognized as good for information security; χ^2=chi-square.							

Table 2:- Information security preparedness indicators

From the findings, it was noted that compliance (50%) and server and network security (50%) were mostly implemented and reviewed on regular basis and recognized as good for information security. This was then followed by data security (35%); security awareness, training and education (35%); system software security (32%); physical and environmental security (30%).it was noted that Information security policy (15%) was the least implemented.

This implies that all technological, environmental and organization controls directly contribute to organization information security and that their individual implementations level affects the security posture of an organization(Ahmad & Mohammad, 2012).

- *Correlation Analysis*

The analysis to determine the nature of relationship that existed between technological controls, Technological Controls, Organization Controls and Information Security Preparedness was computed using Pearson correlation which was tested at 0.01 Alpha Level against 1% level of significance. The findings are presented in a matrix table 2

		Information Security Preparedness
Technological Controls	Pearson Correlation	.623**
	Sig. (2-tailed)	.000
	N	40
Organization Controls	Pearson Correlation	.854**
	Sig. (2-tailed)	.000
	N	40
Environmental Controls	Pearson Correlation	.868**
	Sig. (2-tailed)	.000
	N	40

Table 31:- Correlation Analysis Matrix

The study proved that there exist a positive and statistically significant relationship between technological controls and information security preparedness at 1% level of significance (r= 0.623; p<0.01). This implies that when measures relating to system software, security safeguarding, technological controls, network security and server security safeguarding are implemented in an organization, information security preparedness will be high. Moreover, there exist a positive and statistically significant relationship between Organization Controls and information security preparedness at 1% level of significance (r= 0.854; p<0.01). This mean that when human resource security safeguarding measures, information security policy and awareness creation, training and education are implemented, it will improve on information security preparedness of the organization(Keung, 2014). In addition, it was observed that there exist a positive and statistically significant relationship between environmental controls and information security preparedness at 1% level of significance (r= 0.868; p<0.01). This mean that when all relevant legislative, regulatory or contractual requirements related to security as well as physical and environmental security are implemented in the organization, information security preparedness level will also be improved (Alkalbani et al., 2014).

- *Regression Analysis*

In developing the model weights, multiple linear regression analysis was used to predict information security preparedness using the following equation:

$Y=C+\beta_1X_1+ \beta_2X_2+ \beta_3X_3+$ □

The model summary of the analysis is presented in table 3.

Model	**R**	**R Square**	**Adjusted R Square**	**Std. Error of the Estimate**
1	.949[a]	.900	.891	.21184
a. Predictors: (Constant), Environmental Controls, Technological Controls, Organization Controls				

Table 4:- Model Summary

The model indicates that 90% of the variation of information security preparedness is explained by Environmental Controls, Technological Controls and Organization Controls. This model leaves only 10% as unexplained variation which could be explained by factors outside the study variables.

- *Model Significance*

Model significance is tested using F –statistic shown in table 4.

ANOVA[a]						
Model		**Sum of Squares**	**df**	**Mean Square**	**F**	**Sig.**
1	Regression	14.503	3	4.834	107.731	.000[b]
	Residual	1.615	36	.045		
	Total	16.119	39			
a. Dependent Variable: Information Security Preparedness						

Table 5:- F-statistics

It was established that at 0.05 Alpha Level, against 5% level of significance, the p value=0.000; p<0.05 implies that the model predictors were significant in predicting information security preparedness.

- *Model Weights*

The regression weights were computed as shown in table 5.

Model	Unstandardized Coefficients		Standardized Coefficients	T	Sig.	Collinearity Statistics	
	B	Std. Error	Beta			Tolerance	VIF
(Constant)	-.693	.214		-3.239	.003		
Technological Controls	.141	.072	.126	1.949	.059	.671	1.491
Organization Controls	.577	.096	.448	5.997	.000	.498	2.008
Environmental Controls	.569	.082	.506	6.965	.000	.528	1.894
a. Dependent Variable: Information Security Preparedness							

Table 6:- Coefficients[a]

The findings show that Organization Controls influences 57.7% of Information Security Preparedness and followed by Environmental Controls which influences 56.9%. Finally, Technological Controls influences 14.1% of Information Security Preparedness. VIF statistics was used to measure the presence of multi-collinearity among predictor variables.

V. CONCLUSION

The alarming facts related to e-governance success in Kenya, point to existent inadequacies and inefficiencies in regards to information security practices employed to secure e-governance systems. An extensive survey of literature and existing information security practices adopted by the governments, revealed that the Kenyan government have invested heavily in technical and non-technical measures to protect and preserve their information systems, however have failed to regularly review and update their Analysis of the data collected from the respondents of the study shows that technological, environmental and organization controls directly contribute to organization information security and that their individual implementations level affects the security posture of an organization. Therefore, routine evaluation of these measures results to enhanced organization security hence building confidence and trust in e-governance systems.

VI. REFERENCES

[1]. Ahmad, W. Al, & Mohammad, B. (2012). Can a Single Security Framework Address Information Security Risks Adequately? *International Journal of Digital Information and Wireless Communications*, *2*(3), 222–230.

[2]. Alkalbani, A., Deng, H., & Kam, B. (2014). A Conceptual Framework for Information Security in Public Organizations for E-Government Development. *25th Australasian Conference on Information Systems*.

[3]. Bisandu, D. B. (2016). Design Science Research Methodology in Computer Science and Information Systems. *International Journal of Information Technology*, *November 2016*, 1–6.

[4]. Cisco. (2017). *Cisco cyber security Anual report*. Kenya: Cisco.

[5]. Heitkötter, H., & Majchrzak, T. A. (2013). Design Science at the Intersection of Physical and Virtual Design. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* (Vol. 7939, Issue April 2016). https://doi.org/10.1007/978-3-642-38827-9

[6]. Karokola, G. R. (2012). *A Framework for Securing e-Government Services The Case of Tanzania* (Issue 12). Stockholm University

[7]. Masau, F., Cheruiyot, W., & Mushi, C. (2011). *Trust and its challenges facing E-Government programs in Kenya*.

[8]. Meiyanti, R., Utomo, B., Sensuse, D. I., & Wahyuni, R. (2019). E-Government Challenges in Developing Countries: A Literature Review. *2018 6th International Conference on Cyber and IT Service Management, CITSM 2018*, *April 2019*. https://doi.org/10.1109/CITSM.2018.8674245

[9]. Miah, S. J., & Genemo, H. (2016). A Design Science Research Methodology for Expert Systems Development. *Australasian Journal of Information Systems*, *20*, 1–29. https://doi.org/10.3127/ajis.v20i0.1329

[10]. Nadu, T. (2013). *E-Governance : A move towards paperless Administration in India*. *4*, 404–411.

[11]. Ochara, N. M. (2008). Emergence of the eGovernment artifact in an environment of social exclusion in Kenya. *The African Journal of Information Systems*, 18-43.

[12]. Otero, A. R. (2014). *An Information Security Control Assessment for Organization*. Nova Southeastern University.

[13]. Scarfone, K., & Orebaugh, A. (2008). *Technical Guide to Information Security Testing and Assessment Recommendations of the National Institute of Standards and Technology*.

[14]. Shareef, S. M. (2016). Enhancing Security of Information in E-Government. *Journal of Emerging Trends in Computing and Information Sciences*, *7*(3), 139–146.

[15]. Smith, R. K. (2015). Chapter 2 -Some Well Known Software Development Life Cycle Models. In *Software Development Life Cycle Models* (pp.1–15).http://www.scribd.com/doc/21390992/Chapter-2-Software-Development-Life-Cycle-Models

[16]. UN Department of Economic and Social Affairs. (2016). *E-government Survey 2016*. United Nations.http://unpan1.un.org/intradoc/groups/public/documents/UNDPADM/UNPAN038853.pdf

[17]. Wamoto, F. O. (2015). E-government Implementation in Kenya, an evaluation of Factors hindering or promoting e-government successful implementation. *International Journal of Computer Applications Technology and Research*, *4*(12), 906–915.