IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

THE SITUATION OF INFORMATION TECHNOLOGY SECURITY POLICY IN UNIVERSITIES IN KENYA

Authors

1) Dr. Charles Ochieng' Oguk

2) Mr. Stephen Ochieng' Oguta

ABSTRACT

Despite assertion by many scholars that IT security is instrumental in the management of system security, existing studies hardly delve into the adoption, sensitization and implementation IT security policy in organizations. This survey conducted in the context of universities in Kenya aimed to assess the: availability of IT security policy, IT security training and policy sensitization, and levels of implementation of IT security policy's KPIs. Questionnaires were used to collect data from university staff members, then the data was analyzed using Microsoft Excel to yield frequencies which were expressed into percentages for ease of understanding. Results showed that while IT security policy is vital in system security management, many universities have not adopted it. Further, many staff members are neither trained, nor sensitized on IT security policy. Therefore, it is recommended that IT security policy with relevant KPIs ought to be adopted in all universities, staff trained and sensitized on the security policy for better information systems security management.

Keywords: IT security policy, information systems, policy trainin and sensitization.

INTRODUCTION

Today, universities all over the world rely on information systems for automating their administrative and academic operations. Globally, regionally and in Kenya, management of security of Information Technology (IT) systems in universities is a major challenge. While many universities in Kenya have suffered IT security incidents, which compromise confidentiality, integrity and availability of information systems in different ways; most cases go unreported. Okibo and Ochiche (2014) noted that employees and students of a public university in Kenya used the internet to hack into the university's database, and compromised its integrity by altering examination results, thus affecting graduation that had been scheduled. The interruption of graduation elicited legal suits from the affected students, mounting legal liabilities to the institution. This further stresses the need for proper policy controls and proactive measures against information security breaches in the universities in Kenya. Most universities in Kenya have reported multiple cases of compromising information CIA. However, recent concerns attribute IT security management to IT security policy implementation within the universities, (Makori, 2013).

Statement of the Problem

Universities in Kenya just like elsewhere worldwide, experience various IT security challenges which have been attributed to weak and inadequate implementation of IT security policies. IT security policies should be properly constituted and implemented in order to adequately control the users' and system administrators behavior in universities. However, related contemporary studies have hardly focused on IT security policy training, sensitization and the implementation levels of the policy's PKIs. There is a need to assess both the inclusion of the above PKI of IT security policy and the their levels if implementation within universities in Kenya.

Objectives

i. To assess the availability of IT security policy in universities in Kenya
ii. To assess IT security training and policy sensitization in universities in Kenya
iii. To assess the levels of implementation of IT security policy KPIs in universities in Kenya

LITERATURE REVIEW

Bulgurcu, Cavusoglu and Benbasat (2010) reviewed that IT Security Policy is one of the most critical elements of an organizational IT security program. The study explained that IT security is a management document that identifies rules, regulations, guidelines and procedures that all persons accessing computer resources must use as reference, in order to ensure confidentiality, integrity, and availability (CIA) of data and resources.

A well written security policy forms the cornerstone of an effective information security structure, Peltier et al., (2005). Doherty, Anastasakis and Fulford (2009) showed that a comprehensively written security policy becomes a formal statement comprising the rules and regulations by which workers, contractors and vendors must abide by when working through an organization's information systems. The IT security policy being a management document prohibits users from unsafe computing practices thus facilitating systems security, (Bishop, 2003). Information technology security policy covers proper risk assessment that helps in exposing the vulnerabilities to information security and adoption of better security controls, (Hu, Hart, & Cooke, 2012). Bishop (2003) noted that password implementation, expiry management and privacy form key features of information technology security policy, that ensures data confidentiality and integrity. IT security policy should be considered a major element of information technology security since data security controls like encryption and back-ups, together with network security controls like firewalls, IDS, IPS and VLANs are usually incorporated in the security policy, (Bulgurcu, Cavusoglu, & Benbasat, 2010).

However, implementation of information systems security requirements remains a challenge that makes many institutional information systems' security to be easily compromised, (Huber, Flynn & Mansfield 2016). A study was conducted in universities Minnesota and revealed that the universities continue to suffer from malware attack in their IT infrastructure, due to lack of, or poor implementation of IT security policies (Siponen & Vance, 2010). According to Eira and Rodrigues (2009), universities networks are frequent sources of malware, and as such, properly implemented policies are necessary to ensure better malware management. Jagadeeshwar, Shriramoju and Babu (2016) shows that effective information security policies have coped with malware infestation caused by increased use of mobile computing devices within universities in Ethiopia. Deceulaer (2016) successfully confronted malware menace in private university in Uganda, and devised the use of IT security policy as a non-resource intensive way of controlling malware within a university. Sandvik (2016) found that malware causes multiple losses to information resources and it is a major contributor to system unavailability within learning institutions in Rwanda. It noted that apart from the use of anti-malware, like anti-virus systems, well implemented IT security policy, especially on user training helps in managing malware.

In South Africa, malware's adverse effects within institutional information systems' infrastructure raised much concerns to the extent that a supervised comparative study and analysis of attack methods for malware and IT policy control was proposed, (Kruczkowski & Niewiadomska, 2014). The study concurred with Renaud, Blignaut, and Venter (2016) study which showed that “Bring Your Own Devices” BYODs, like smart-phones not only bring virus into South-African university's computer networks, but are also at risk of being attacked and should therefore is protected using effectively implemented IT security policy. Bessette, et.al, (2015) showed that IT security policy performance indicators should include; proper implementation of the policy, staff sensitization about the policy, and establishment of the rules that guide behavior of IT systems ’users, specification of penalties for violation and meeting

given industry standards' requirements. The PKI constitute the sub-elements of IT security while the involvement of users starting at the policy formulation levels is recommended (Sandvik (2016).

In kenya, a study was conducted by Kimwele et al., (2010) on the implementation of IT policies within Kenya's Small and Medium Enterprises (SMEs). It revealed that over 50 percent of the employees were not informed about unacceptable and acceptable use of information systems' assets of the enterprises. Further Tarus (2015) noted that in universities, students' finance, students' registration, examinations, human resources, internal audit, library, and computer laboratory are the operation areas of IT systems in the universities in Kenya. This view was supported by Ndung'u (2015) study indicated that most staff members in the operation areas have embraced information technology and use it at their places of work.

The preceding studies reiterate that IT security policy is so important that it should be incorporated in development of information systems security measurements of status. In the international spectrum, regional level as well as in Kenyan local levels the foregoing studies have attributed information security breaches to inadequate implementation of IT security policies in the institutions, and further highlighted key performance indicators (KPI) for IT security policy to include: proper implementation of the policy, staff sensitization about the policy, establishment of the rules that guide behavior of IT systems' users, specification of penalties imposed on users upon violation of the policies and meeting given industry standards' requirements.

The study gap

Despite the above studies highlighting KPIs for IT security policy, studies have hardly focused on the key aspects of IT security policy, especially: the aspects of training, sensitization and the implementation levels of the PKIs. There is a need to assess both the inclusion of the above PKI of IT security policy and the their levels if implementation within universities in Kenya.

METHOD

Mixed sampling approach was adopted in this study. The universities were first stratified as public and private universities, then ten percent random sampling was applied on each strata to yield seven (7) universities as composed on the table below.

The university population and the sample

University category	Total Number	Sample sizes (@ 10 %)
	Stratified Sampling	**Simple-Random Sampling**
Public universities	33	3
Private universities	37	4
Total	70	7

With thirteen (13) operational areas (as backed by studies) being purposively sampled for the already sampled seven universities, the total sample size was (13 x 7 = 91 respondents), as drawn in the table below.

Purposive Sample sampling

Operation Area (Category)	No of team leader(s)	No of universities	Sample size per category
IT leadership	1	7	7
Systems administration	1	7	7
Network administration	1	7	7
Security administration	1	7	7
DB administration	1	7	7
Students' finance	1	7	7
Students registration	1	7	7
Examinations	1	7	7
human resources	1	7	7
Internal Audit	1	7	7
Library	1	7	7
Computer Lab	1	7	7
Students Leadership	1	7	7
Totals	**13**	**(13X7)**	**91**

From the sample, well designed questionnaires were used to collect data with regards to each objective. Data was then analyzed using SPSS software and Microsoft Excel to yield pertinent statistical values addressing the given objectives of the study.

RESULTS

Information Technology Security Policy

This study revealed that up to 63 percent of the universities have IT security policy in place. However, 37 percent of the respondents indicated that they do not have the policy. This implies that that access and use of information systems' resources are not well guarded in 37 percent of the universities. If up to 37 percent of universities in Kenya have not adopted IT security policy, it is such a substantial level that need to be addressed. This finding, where a substantial number of universities lack IT security policy does not agree with (Kimwele et al., 2010), which portrayed security policy as a high level document, usually associated with top management that stipulates the goals and constraints for using IT system, and as such ought to be part of any university. The current study shows that even within the universities where information systems have been adopted and implemented, recognition of IT security policy is not yet fully entrenched among the personnel. For instance, the results indicated that only accumulation of 32 percent of the respondents agreed that IT security policy is implemented effectively and the staff members sensitized about it

The findings further indicate that up to 40 percent of the respondents do not feel any great impact of the information technology security policy in the universities. The study finding is a departure from the studies reviewed in the literature that portray information technology security prohibits users from unsafe computing practices, thus facilitating systems security (Bishop 2003). This implies that computing practices that should be restricted by the use of information technology security policy are hardly controlled within some of the universities in Kenya. Further confirmed is that 60 percent of the respondents felt that the IT security policies in their universities do not effectively guide the behavior of the users of information systems. Further findings showed that among the systems users, 47 percent of the users do not know the policy guidelines on sharing system access passwords, while over 51 percent of the users are unaware of any consequences for violating IT security policy. This implies that despite the presence of information technology security policy in some of the universities, violators of the policy do not face any consequence, hence such penalties remain unknown.

Over 64 percent of users are never trained regularly on IT security requirements, while only 42 percent are sensitized on the safe computing practices. Casey, (2011), stresses the achievement of information technology security through implementation of information security policies that involves providing training and sensitization on it. However, over 60 percent of the respondents showed that universities had not implemented IT security policy and sensitized the staff effectively. The inadequate levels of implementing the policy could be attributed to the increasing incidents of systems breach within the universities today. The poor implementation of information technology security policy is a deviation of the requirement and expectation of the above studies and could adversely affect the organizations information systems' security. The study further indicated that 72 percent of the respondents confirm that consequences of violating the policy are not effectively spelt out, while only 28 percent of the respondents confirm that the consequences are well spelt out. This generally implies that 72 percent of the university staff across the country is not aware of the IT policy requirements. The finding agrees with a study conducted by Kimwele et al., (2010) on the implementation of IT policies within Kenya's (SMEs) and revealed that over 50 percent of the employees were not informed about unacceptable and acceptable practices for information systems'.

Percentage level of adoption of IT security policy elements within the universities

	V. Ineffective	Ineffective	M. Ineffective	Effective	V. effective
Level of implementation	20	20	28	20	12
consequences for violation	12	28	32	16	12
meets industry requirements	16	36	20	16	12
Guides IT users behavior	20	20	20	12	28

52 percent of the respondents showed that the policy does not effectively meet the industry requirement, while only 32 percent of the respondents showed that it does. The current study also indicated that up to 52 percent of the

universities have adopted information systems' security policies that hardly meet the industry standards. Policies with dispersed conformance from the standards are unreliable and my not offer adequate safeguards and guidelines to information technology security management. This finding is supported by Makori (2013) findings that there are gaps between IT security practices and the industry requirements in universities in Kenya.

CONCLUSIONS

The study found that while IT security policy plays an important role in IT security management, it is still inadequately implemented in the universities in Kenya. This is because some of the universities still do not have the policy in place while those that have, not all of them do implement it adequately.

RECOMMENDATIONS

It is evident from the study that the implementation levels of IT security policy is still inadequate within universities in Kenya. The study therefore recommends adoption of all IT security policy in all the institutions and improvement on the policy implementation therein.

Appendices

QUESTIONNAIRE

Do you have an IT security policy? Yes [ ] No [ ]

Is there functional IT security policy in the university? Yes [ ] No [ ]

To what extent do you feel the impact of IT security policy?
low [ ] Moderate [ ] High [ ]
Do you know what the IT security policy requires on sharing user password?
Yes [ ] No [ ]
Are there well defined consequences for violating IT security policy?
Yes [ ] No [ ]
How often does the university train you on IT security?
Regularly [ ] Irregularly [ ] Never [ ]
Are employees sensitized on IT security requirements and practices?
Yes [ ] No [ ]

Is there IT security training and awareness program /policy for employees?
[ ] Yes [ ] No

levels of implementation of IT security policy KPIs in universities (scale of 1-5)

	Element one: **IT security Policy**					
		1	*2*	*3*	*4*	*5*
		Scale				
	Policy is implemented and staff sensitized about it?					
	Policy meets the industry standards' requirements?					
	Policy specifies the consequences for violation?					
	Policy establishes the rules that guide behavior of users?					

REFERENCES

Bessette, D., LeClair, J. A., Sylvertooth, R. E., & Burton, S. L. (2015). Communication, Technology, and Cyber Crime in Sub-Saharan Africa. *New Threats and Countermeasures in Digital Crime and Cyber Terrorism*, 286

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS quarterly*, *34*(3), 523-548.

Bishop, M. (2003). What is computer security?. *IEEE Security & Privacy*, *1*(1), 67-69.

Deceulaer, D. (2016). Securing a school network and making it malware-free with limited resources: based on my experience in Mountains of the Moon University.

Doherty, N. F., Anastasakis, L., & Fulford, H. (2009). The information security policy unpacked: A critical study of the content of university policies. *International Journal of Information Management*, *29*(6), 449-457

Eira, J. P., & Rodrigues, A. J. (2009). Analysis of WiMAX data rate performance. Lisbon: Instituto de Telecomunicaçõ̃es/Instituto Superior, Technical University of Lisbon.

Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing employee compliance with information security policies: The critical role of top management and organizational culture. *Decision Sciences*, *43*(4), 615-660.

Huber, K. D., Flynn, J. J., & Mansfield, W. G. (2016). *U.S. Patent No. 9,319,964*. Washington, DC: U.S. Patent and Trademark Office.

Jagadeeshwar, M., Shriramoju, S. K., & Babu, A. R. (2016). Optimal Distributed Malware Defense in Mobile Networks with Heterogeneous Devices.

Kimwele, M., Mwangi, W., & Kimani, S. (2011). Information technology (IT) security framework for Kenyan small and medium enterprises (SMEs). *Int. J. Comput. Sci. Secur. IJCSS*, *5*(1), 39.

Kruczkowski, M., & Niewiadomska-Szynkiewicz, E. (2014). Comparative study of supervised learning methods for malware analysis. *Journal of Telecommunications and Information Technology*, (4), 24.

Makori, E. (2013). Adoption of radio frequency identification technology in university libraries: A Kenyan perspective. *The Electronic Library*, *31*(2), 208-216.

Ndung'u, P. W., & Kyalo, J. K. (2015). An evaluation of enterprise resource planning systems implementation experiences for selected Public Universities in Kenya.

Okibo, B. W., & Ochiche, O. B. (2014). Challenges Facing Information Systems Security Management in Higher Learning Institutions: A Case Study of the Catholic University of Eastern Africa-Kenya. *International Journal of Management Excellence*, *3*(1), 336-349.

Peltier, T. R. Tich, r.e, Yae, U., Polkh, w.(2005). Implementing an Information Security

Awareness Program. *Information Systems Security*, *14*(2), 37-49.

Renaud, K., Blignaut, R., & Venter, I. (2016). Smartphone Owners Need Security Advice.

Sandvik, K. B. (2016). The humanitarian cyberspace: shrinking space or an expanding frontier?. *Third World Quarterly*, *37*(1), 17-32.

Siponen, M., & Vance, A. (2010). Neutralization: new insights into the problem of employee information systems security policy violations. *MIS quarterly*, 487-502.

Tarus, J. K., Gichoya, D., & Muumbo, A. (2015). "Challenges of implementing e-learning in Kenya: A case of Kenyan public universities". *The International Review of Research in Open and Distributed Learning,* 16(1).