American Journal of Humanities and Social Sciences Research (AJHSSR)
e-ISSN :2378-703X
Volume-3, Issue-6, pp-241-245
www.ajhssr.com
Research Paper Open Access

Towards an Information Security Maturity Model for Universities Based On ISO 27001

Daniel Makupi[1], Simon M. Karume[2]
[1](*Department of Information Technology Security, School of Computer Science and Bioinformatics, Kabarak University, Kabarak, Kenya)*
[2](*Department of Mathematics & Computing Science,Laikipia University, P.O. Box 1100 – 20300, Nyahururu, Kenya)*

ABSTRACT : Information infrastructure is one of the most important assets in universities. With rapid advancement in technology, it poses a challenge as adversaries have come up to attack information and information systems. Most of the Information security attacks are normally targeted to organizations unaware coupled with the fact that most of the higher educational institutions are not aware of their information security posture. Therefore measuring the level of security of an organization would be vital in preparedness towards information security. In this paperthe study proposes a framework for assessing university information security maturity status. The said framework will take into consideration ISO 27001 by involving specific clauses relevant to universities. The cumulative factors contributed from risk domains can then be used for computation of information maturity.

KEYWORDS: *Security, maturity, framework, ISO 27001*

I. INTRODUCTION

The need for organizations to adopt information security so as to thrive in today's business environment that is highly technical is indisputable. According to report from the Open Security Foundation, 15% of data breaches since records began have happened in educational institutions (Park, &Ahn, 2017). These places especially higher education establishment's face a unique set of challenges that makes it different from non-academic institutions (Zhou et al, 2017).

Many of these challenges facing universities are intimately bound together because of highly independent activities and incongruent service and applications sharing framework (Swanson, & Vogel, 2018). The network implementation approach in universities is often sophisticated and intricate (Avena et al 2018). This, in turn, is a result of higher education's idiosyncratic organizational structure (Liu et al, 2017). A majority of universities have lots of separate independent networks that are firewalled off from one central location.

Openness is also one of the educational sector's biggest weaknesses from a cyber-security standpoint, but it is also one of its saving characteristics (Obama, 2010). That's one of the unique attributes of higher education: in general, but especially around the topic of information security, higher education establishments share information (Blumenthal et al, 1996). Sharing information between academic institutions to establish and reinforce best practices is a key part of university process.

The university wide technology culture is decentralized in terms of leadership, decision-making, and IT infrastructure (Katz, & Townsend, 2000). Private sector organizations operate at varying levels of cohesion; the employees in them, for the most part, work toward a common goal. Conversely, a university isn't so much an institution as a set of loosely coupled functions (Brown, &Duguid, 1998). It employs some people, but is paid by others for the privilege of conducting research. It is a squirming bag of political and economic relationships (Robison, & Ritchie, 2016).

This inherent looseness of university technological implementation framework creates challenges not only in technical infrastructure, but also in their effort to offer quality services to learners and researchers of different cadre (Alavi, &Leidner, 1999). According to EduCASE report (2017), "Adversaries however have come up to disrupt operations in educational institutions because of the critical nature and financial value of information and information technology assets attached to its operations".

Most of the Information security attacks are normally targeted to universities with the fact that most of them are not aware of their security posture. According to report by serianu group (2016), "cybercriminals are deliberately targeting Kenyan organizations with the intention of wreaking havoc and making away with millions. Hackers collectively invest in their own expertise and tools to hack siloed and non-forward looking

institutions who continue to ignore this phenomenon". This can be attributed to lack of industry specific measure of information security maturity (Qu, 2011). To compound the problem, both students and tutors like to bring in their own devices, and the explosion of post-PC hardware over the last two years has exponentially expanded the number of platforms (Yeap, 2013). End points are notoriously leaky, and can not only bleed information out of a network, but can leak malware back in.

Despite the disruption of information and information technology which has very high negative financial and reputational damage there's no benchmark on when a security infrastructure improvement or countermeasures can be deemed appropriate (Schellong, 2010). In addition there has not been a mechanism in place in form of a model to come up with the maturity level of information security in universities to serve as guidance for security awareness and readiness indicator (Hsu, 2012).

1.2 Statement of the Problem

The need for a framework to assess the information security maturity of a universe due to exasperating and widening gap between awareness and information infrastructure investment. Organizations operate in a silo like manner unaware of their maturity in information security. Often when online attacks and fraud do happen that's the time an organization gets to understand they had vulnerability. The aftermath of fraud, they end-up spending heavily on forensic audit and investigations. In addition, there has not been a mechanism in form of a model to cumulatively come up with the threshold inform of status level as a result of risk exposure by organizations, therefore, this research will serve to inform the status level of information security maturity.

1.3 Research Objective

Our main focus is to come up with a framework that would aid universities to measure their maturity in information security by commutatively considering risks facing the individual organizations. Maturity status will serve to appropriately inform the security posture of the organization.

II. LITERATURE REVIEW

Information Security Maturity level is the measurement of organization's capability to remain secure (Dzazali, 2006). Information technology is a very important requirement for all enterprise organizations today because it is proved to help in improving the effectiveness and efficiency of enterprise business processes (Surni& Nina, 2015).The information security maturity model (ISMM) is a tool to evaluate the ability of organizations to meet the objectives of security, namely, confidentiality, integrity, and availability while preventing attacks and achieving the organization's mission despite attacks and accidents (Suwito, et al, 2016). The model defines a process that manages, measures, and controls all aspect of security. It relies on four core indicators for benchmarking and as an aid to understanding the security needs in the organization. These indicators are goal-driven to achieve the security needs **(**Malik, 2011).

The critical information security risks that are critical to universities originate from human behavior. People are regarded as the greatest weakness of Information Security according to (Mitnick& Simon, 2003; Silva & Stein, 2007; Sêmola, 2014). For this reason, information protection should not be only a technical issue, but also social, for which there is no purely technological solution known.Therefore, measures towards information security should not only address technological and physical issues but also administrative, to change human behaviour in the organization. Curry et al (2005) proposes to classify Information Security measures as they aim to affect educational institutions and industry.

According to Belasco and Wan (2006) and ABNT (2005) suggest various administrative, technical and physical measures. Although some of them are widely adopted, such as the use of firewall, antivirus, anti-spam, logical access control, proxy, the existence of Information Security Policy, incident treatment team, backup routines, the use of uninterruptible power supply (UPS) and a safe box to store media, Sêmola (2014) warns that each organization has its own characteristics, and that this leads to particular needs of Information Security. Dresner (2011) agrees and adds that the simple adoption of measures proposed by standards and models does not guarantee the mitigation of risks.

III. PROPOSED FRAMEWORK

The framework that will aid in the implementation of the model to compute information security maturity of a university based on ISO 27001 is as shown below in Fig 1

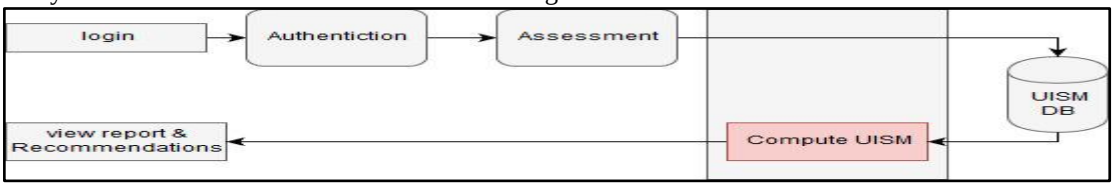

Fig 1: Web based Framework for computing information security maturity (source: Author)

The operation of the framework is such that it will enable the users to be registered and consequently login to access the system. Once the user accesses the system depending on the need of the user as such could be a university who may want to compute their information.

3.1. Framework Operation

A scientific model proposed for the computation of information system security (ISMS) maturity of a university is a shown below. The consideration of factors that determines the security maturity is based on the security benchmark standard ISO/IEC 27001. It considers relevant clauses of the security standard applicable to a university.

University Information Security Maturity (UISM) will be computed using the formula;

Equation 1 UISM formula derivation

$UISM = R_1W_1 + R_2W_2 + R_3W_3 + \ldots\ldots\ldots\ldots\ldots\ldots R_nW_n$

Therefore;

$USIM = \sum_{i=1}^{n}(W_iR_i)$

Where; $W_1, W_2, W_3 \ldots\ldots\ldots\ldots W_n$,respectivelyare the weights that can be determined through focusing group discussion by this study.

While; $R_1, R_2, R_3 \ldots R_n$ respectively are the weighted indicators that will determine the state of a particular risk security factor.The weights will be such it will be rated has; not performed, performed in formerly, planned, well defined, quantitatively performed and continuously improving according to ISO/IEC 21827:2008 maturity standard. Once the weighted scores are obtained from the focus groups associated with each security factor then the university information security maturity (UISM) can be computed.

The model works in the premise that the cumulated factors and its combined indicators will determine the maturity level of information security in universities. Security risk factors are weighted according to the level of maturity in the university. The maturity level will be determined by considering the different clause in the ISO/IEC 27001 proposed has independent factors in the metrics development. Below is a summary of the focus of each section used that will be included in the model:

i. **Administrative controls**
   a. Information Security Policies (ISO 5): Assess how an institution expresses its intent with regard to information security.
   b. Human Resource Security (ISO 7): Assess an institution's safeguards and processes for ensuring that all employees are qualified for and understand their roles and responsibilities of their job duties and that access is removed once employment is terminated.
   c. Compliance (ISO 18): Assess an institution’s processes for staying current with legal and contractual requirements to protect sensitive information assets.

ii. **Technical controls.**
   a. Cryptography (ISO 10): Assess an institution's policies on the use of cryptography (encryption) and key management.
   b. Communications Security (ISO 13): Assess an institution’s formalized policies, procedures, and controls, which assist in network management and operation.
   c. Access Control (ISO 9): Assess an institution’s use of administrative, physical, or technical security features to manage how users and systems communicate and interact with other information resources.

iii. **Physical Controls**
   a. Physical and Environmental Security (ISO 11): Assess an institution's steps taken to protect systems, buildings, and related supporting infrastructure against threats associated with their physical environment.
   b. Information Security Aspects of Business Continuity Management (ISO 17): Assess an institution’s business continuity management. A mature institution has a managed, organized method for the development of procedures to ensure the continuity of operations under extraordinary circumstances including the maintenance of measures to ensure the privacy and security of its information resources.
   c. Asset Management (ISO 8): Assess an institution's asset management program. Does it include ways to identify, track, classify, and assign ownership for the most important assets to ensure they are adequately protected?

Upon consideration of the above ISO/IEC clauses has a function and product of factor on the individual weight then we can therefore come up with a university information system security maturity (UISM).

IV. RECOMMENDATION

The proposed system can present a number of advantages towards assessing information security maturity, these are:

- *Capture of user detail*: these details will be captured once, used many times and can be shared to other incidental utilizations.
- A *system that's easy*: the utilization of the Web based model for computation of information security maturity will make it very easy to use.
- *Operation affordability*: the use of the Web based model will be relatively low cost because multiple users will connect to a common system.
- *Generation of report:* in implementing the framework it will make it possible to produce summary reports of maturity in information security. This information is often not availably and accurate in the present setup that relies on manual records.

4. 1 Challenges

The main concern that will be of challenge especially to the universities is ensuring trustworthiness and provision of information truthful to reflect the actual position in information security maturity. Some of universities my not be willing to have third party auditing organization to assessing their information security maturity.

V. CONCLUSIONS

This concept, therefore, envisions this approach of using a framework that automatically upon considering ISO 27001 risk checklist it automatically computes the security maturity of an organization. In its working the system will go hand in hand in appropriately informing the universities on areas to invest and appropriate defence in-debt strategy to ensure confidentiality, integrity and availability.

VI. AREAS FOR FURTHER STUDY

The proposed framework can also be utilized by government and other interested players in considering fraud exposure indexes of higher learning institutions and in these context universities and also advising appropriately by coming with relevant laws to ensure universities adhere to and are up-to-date in ensuring their infrastructure security.

REFERENCES

[1.] Park, W., &Ahn, S. Performance comparison and detection analysis in Snort and Suricata environment. *Wireless Personal Communications*, *94*(2), 2017, 241-252.

[2.] Zhou, J., Cao, Z., Dong, X., &Vasilakos, A. V.Security and privacy for cloud-based IoT: Challenges. *IEEE Communications Magazine*, *55*(1), 2017, 26-33.

[3.] Swanson, M. H., & Vogel, K. M.Big Data, intelligence, and analyst privacy: investigating information dissemination at an NSA-funded research lab. *Intelligence and National Security*, *33*(3), 2018, 357-375.

[4.] Avena-Koenigsberger, A., Misic, B., &Sporns, O.Communication dynamics in complex brain networks. *Nature Reviews Neuroscience*, *19*(1), 2018, 17.

[5.] Liu, C. W., Huang, P., & Lucas, H.IT Centralization, Security Outsourcing, and Cybersecurity Breaches: Evidence from the US Higher Education. (2017).

[6.] Obama, B. *National security strategy of the United States (2010)* (Collingdale, PA: Diane Publishing, 2010).

[7.] Blumenthal, D., Causino, N., Campbell, E., & Louis, K. S.Relationships between academic institutions and industry in the life sciences-an industry survey. *New England Journal of Medicine*, *334*(6), 1996, 368-374.

[8.] Katz, J., & Townsend, J. B.The role of information technology in the" Fit" between culture, business strategy and organizational structure of global firms. *Journal of Global Information Management (JGIM)*, *8*(2), 2000, 24-35.

[9.] Brown, J. S., &Duguid, P. Organizing knowledge. *California management Review*, *40*(3), 1998, 90-111.

[10.] Robison, L. J., & Ritchie, B. K.*Relationship economics: The social Capital Paradigm and its Application to business, politics and other transactions.* (Florida: CRC Press, 2010).

[11.] Alavi, M., &Leidner, D. E.Knowledge management systems: issues, challenges, and benefits. *Communications of the AIS*, 1(1), 1999, 1-7.

[12.] Brown, J. S., &Duguid, P.Organizing knowledge. *California Management Review*, *40*(3), 1998, 90-111.

[13.] Robison, L. J., & Ritchie, B. K.*Relationship economics: The social capital paradigm and its application to business, politics and other transactions*.. (Florida: CRC Press, 2016).

[14.] Qu, W. (2011). *A Study of voluntary disclosure by listed firms in China* (Ph. D, Deakin University, 2011).

[15.] Yeap, G. (2013, December). Smart mobile SoCs driving the semiconductor industry: Technology trend, challenges and opportunities. In *Electron Devices Meeting (IEDM), 2013 IEEE International*, 2013, 1-3.

[16.] Schellong, A. R. Benchmarking EU e-government at the crossroads: a framework for e-government benchmark design and improvement. *Transforming Government: People, Process and Policy*, *4*(4), 2010, 365-385.

[17.] Hsu, C., Lee, J. N., & Straub, D. W.Institutional influences on information systems security innovations. *Information systems research*, *23*(3), 2012, 918-939.

[18.] Dzazali, Suhazimah, "Social Factors Influencing the Information Security Maturity of Malaysian Public Service Organization: An Empirical Analysis" (2006). *ACIS 2006 Proceedings*. Paper 103.Electronic version found at http://aisel.aisnet.org/acis2006/103

[19.] SurniErniwati and Nina KurniaHikmawati, ―An Analysis of Information Technology on Data Processing by using Cobit Framework‖, (IJACSA). *International Journal of Advanced Computer Science and Application*, 6(9), 2015, 151 – 157.

[20.] Suwito, M. H., Matsumoto, S., Kawamoto, J., Gollmann, D., & Sakurai, K. An Analysis of IT Assessment Security Maturity in Higher Education Institution. In *Information Science and Applications (ICISA)*, 2016 ,701-713). Springer, Singapore.

[21.] Malik F. S. *Management Information Systems*. (Prince Mohammad Bin Fahd University, Saudi Arabia, 2011).

[22.] Curry, M., Marshall, B., Crossler, R. E., &Correia, J. InfoSec Process Action Model (IPAM): Systematically Addressing Individual Security Behavior. *ACM SIGMIS Database: the DATABASE for Advances in Information Systems*, *49*(1),2018 49-66.