International Journal of Innovative Research and Advanced Studies (IJIRAS)
Volume 7 Issue 10, October 2020

ISSN: 2394-4404

A Framework For Secure University Networks For Effective Business Continuity

Jeremiah Oyana Owango

Anthony Rodgrigues

Samuel Liyala

Department of Computer Science and Software Engineering,
Jaramogi Oginga Odinga University of Science and Technology, Kenya

Abstract: ***In the past few years Kenyan Universities have connected to broadband internet connectivity, which brought great improvement in data communication but created a serious flaw in information security. This has raised concerns due to multiple technologies that allow unlimited connections to university networks. This paper investigates current challenges that affect business continuity in regards to cyber-attack trends with emphasis on data in transmission and storage. A total of 37 respondents from Kenyan Universities participated in this study. The results show there is need to come up with a comprehensive secure solution for information security in Kenyan Universities. This study is significant because it will help in research for a secure framework and enable secure university networks.***

Keywords: Broadband, Business Continuity, Cyber-attack, Data Communication, Framework,

I. INTRODUCTION

The concept of information risk and universities seem irrelevant, universities are viewed as ivory towers isolated and separate from the corporate world, a place for deep thinking and discussing matters of philosophy and generating theories and validating those theories. Therefore, the concept of risks seems irrelevant in such a place. The reality is, however, risk is part of everyday life, (Jarrell et al., 2008) argued, despite their core education mission, universities are more like cities in terms of numbers and variety of services they provide. (Mitroff et al., 2006) states that "as the complexity of institutional operations, technology and infrastructure increases, the risks facing universities and their leaders multiply as well, and wise leaders will plan accordingly" (p. 62). Although the field of crisis management is 20 years old, colleges and universities do not appear to be prepared for major disasters, the risk this study is addressing is cyber threats.

Business continuity plans are considered a risk control, to ensure limited to none downtime in the event of a risk occurring (Cerullo & Cerullo, 2004). Managing cyber threats in universities is problematic, due to the openness and transparency of their networks, with majority of universities lacking business continuity plans, in addition the ECAR study Shelter from the Storm: IT and Business Continuity in Higher Education (Yanosky, 2007) acknowledges that most business continuity plans at higher education institutions are not tested.

Colleges and universities across the Republic of Kenya have realized that they can no longer rely on out-dated, manual processes that hamper productivity and drive up costs hence complete reliance on information technology (Universitybusinessstaff, 2013), specifically with Kenyan Universities being compelled by the government within the framework of Kenya Vision 2030 to introduce e-learning and blended learning as an alternative delivery system to increase accessibility to higher education in Kenya (NESC, 2007). Cyber attacks on African Universities are not regarded as serious issues and are simply bundled up as simple information technology-based problems (Sawahel W, 2017). Cyber-attacks to institutions are growing annually and exponentially, while survivability of affected institutions

getting back online takes longer and longer (Privacy Rights Clearinghouse, 2014). It has been noted many universities now conduct cyber research, and can be a gold mine of information on vulnerabilities, exploits, breaches, and techniques (Giandomenico, 2018), this is in line with (Elmrabi et al., 2015) who stated insider threats being a major source of cyber threats in institutions of higher learning, this was affirmed by (Coughlan, 2018), when a government-funded agency that provides cyber-security examined the timing of 850 attacks between 2017-18 and noted cyber-attacks against universities and colleges in the UK discovered staff or students could often be responsible, rather than organized crime or hacking .groups external to the institution.

Higher education had the highest rate of ransomware attacks among all industries surveyed in a 2016 report published by BitSight (a cyber risk management company), and the second highest rate in BitSight's 2017 report (Campbell, 2017). Due to the fact many institutions of higher learning were so early in adopting digital tools and interfaces (and as a result of financial and other practical concerns) still rely on legacy systems that are particularly vulnerable to attacks (Riddell & Eide, 2016) there are countless intrusion points for intruders to capitalize on. Cyber attackers use cutting edge technologies and methods to exploit university systems that are, in some cases, woefully outdated and outmatched, specifically, university IT systems are often characterized by a decentralized and, in (SecurityNewsDaily, 2012) view, haphazard construction that attackers can easily exploit.

The purpose of this study is to investigate and create a proper understanding of cyber threats in local universities then develop a framework that can offer a comprehensive and adequate secure network environment in Kenyan Universities. This study is significant since the framework created can be used globally in the institution or piecemeal on department, faculties or school level to better secure information technology assets and guide university management form informed decisions on cyber security.

II. LITERATURE REVIEW

A. UNIVERSITY CYBER SECURITY TRENDS

In 2014, 10% of reported security breaches involved cyber-attacks to the education sector (Symantec, 2014), by 2016 of all cyber attacks carried out in learning institutions were affected by 60% of computer virus, 11% successful hacking attempts and 11% successful phishing scams (Mutisia, 2018). In the United States in the first half of 2017, the education sector accounted for 13 percent of data breaches, resulting in the compromise of around 32 million records, this was as a result of malware attacks (Giandomenico, 2018).

The 2017 Serianu Cyber Security Survey shockingly reveals that over 95% of African businesses are operating below the Cyber 'security poverty line (Munyendo et al., 2017), this is not surprising, as trends indicated rise of cyber-attacks to institutions of higher learning due to DNS-based threats rising by 68% (Bayern, 2018). This increase is attributed *to t*he rise in IoT devices and astonishing numbers of BYOD devices, especially among college-age students, leaving universities open to more vectors of attack (EfficientIP, 2018). This trend of increase in insecurity may be due, in part, to the sheer number of personal records kept by these institutions, considering their ever-changing student bodies, as well as the valued open, collaborative environment of most colleges and universities and vast amounts of information technology assets that can be hijacked (Harris & Hammargren, 2016). But it was much harder to establish the extent of financial losses by the public sector. Unlike many governments, Kenya has not established any mechanisms to track and calculate the losses made by public sector organizations to cybercrime. This makes them even more susceptible to such crimes such as website defacements and ransom demands from criminals before restoration, with public universities in the country falling in this category (USIU-Africa, 2015).

B. SECURITY CHALLENGES

The higher education sector ranks highest among the worst business sectors for handling cyber threats, with 73% of instiurions taking three or more days to apply a security patch once a flaw has been detected and security alerts sent out (Bayern, 2018). The largest recurrent cyber threats to university networks are channeled through Bring your Own Devices (BYoD) and Internet of Things (IoT), (Abomhara, M. 2015) which include but not limited to malware, social engineering and network infrastructure attacks where the large networks are compromised and it's cyber resources are utilized to facilitate other attacks, sophisticated DDoS attacks that evolve periodically to en-campus new and different threat attack matrix. (Bradley, 2015), social engineering attacks are biggest threats facing cyber security in universities, (Arana, M. 2017; Chargo, M. 2018; Libicki, M. 2018; Costantino, G et al, 2018; Pavkovi´c & Perkov 2011; Breda, Barbosa, & Morais, 2017). According to (Libicki, M. 2018), they can be detected but difficult to stop. Social engineering also facilitates infiltration of malware that infect the massive network equipment to be hijacked which creates robot networks, botnets for short. The SE-botnet by US group predominantly affects social networks which exploits social engineering attacks to spread bots on social networks, which university networks transmit large amounts of social media traffic. Simulation results demonstrate that the SE-botnet can capture tens of thousands of bots in one day with a great infection capacity (Li et al., 2011). These botnets can be used to commit cyber crime or launch denial of service attacks

C. POLICIES, STANDARDS AND FRAMEWORKS

a. CIA CONFIDENTIALITY, INTEGRITY AND AVAILABILITY TRIAD

The fundamental security principles represented in the CIA triad ensure that both the data and the information system that processes the data are protected. The CIA triad ensures that protection takes place on three levels: the physical, technical and organizational, (Farooq, et al., 2015). Put together, the triad preserves and protects sensitive information,

whether personal or proprietary, (Mosenia, A., & Jha, N. K. 2016) in transit or storage (Greer, C et al, 2014). Unfortunately, in the country their does not exist an act or policy that regulates the transmission of data or data in storage for Government Enterprise Networks (GEN) which universities tend to adopt, because of this universities have a mix of policies that they create and use, which lack uniformity (Aineah, 2017).

Standard/Framework Description	Challenges faced in implementation
ISO/IEC 27001 Standard ISO 2700-x provides a security framework and process accreditation relative to the standards process	- Few institutions of higher learning are iSO 2700-x certified - Lack of guidance in the implementation of the standard -Broad technical skill required for implementation
COBIT	A lack of focus on how to achieve the necessary goals of the COBIT framework Difficult to implement in a large organization. A significant amount of time needs to be set aside to identify and create all the steps needed in order to fully realize the COBIT framework.
NIST Security framework. Contains the controls required for information security	Not focused on market or financial gains. Does not offer worldwide certifications Needs an in depth understanding of security control for implementation. Suits large governmental organizations

Table 1: Standards and Framework

D. LAWS AND REGULATIONS

CURRENT LAW ON CYBER SECURITY IN KENYA: Currently, Kenya has no overarching law that focuses on such incidents of cyber security, but the Kenya Information and Communication Act of 1998 (KICA) includes cyber security related provisions that prohibit various actions that would threaten cyber security and prescribes criminal penalties for the same, there also exists cybercrimes and computer misuse act 2018, that had been suspended but fully implemented in 2020.

PROPOSED LAW ON CYBER SECURITY IN KENYA: Although the provisions of the KICA are useful in the war against cybercrime, plenty remains to be done at legislative and policy levels in order to help stem the tide of cyber-attacks. The Cyber Security and Protection Bill 2016, which was gazette in 2016 is yet to be tabled before Parliament (Okoth & Ojango, 2019).

E. CONCEPTUAL FRAMEWORK

The independent variables are the information security attributes of Administrative, Physical and Logical controls in relation to securing university networks which is the dependent variable.

The unique cyber environment found in universities include campuses being dispersed over large geographical area, an enormous student population, faculty staff collaboration in research with other institutions stems from the organization culture unique to universities making this variable the cause of unusual cyber security mechanisms adopted by universities making it a moderator variable. The security infrastructure adopted by institutions depends on whether the type of security mechanism chosen will influence or moderate how cyber threats would affect an institutions business process and the severity of an attack and how capable and efficiently an institution would continue delivery of services at acceptable predefined levels following a disruptive incident.

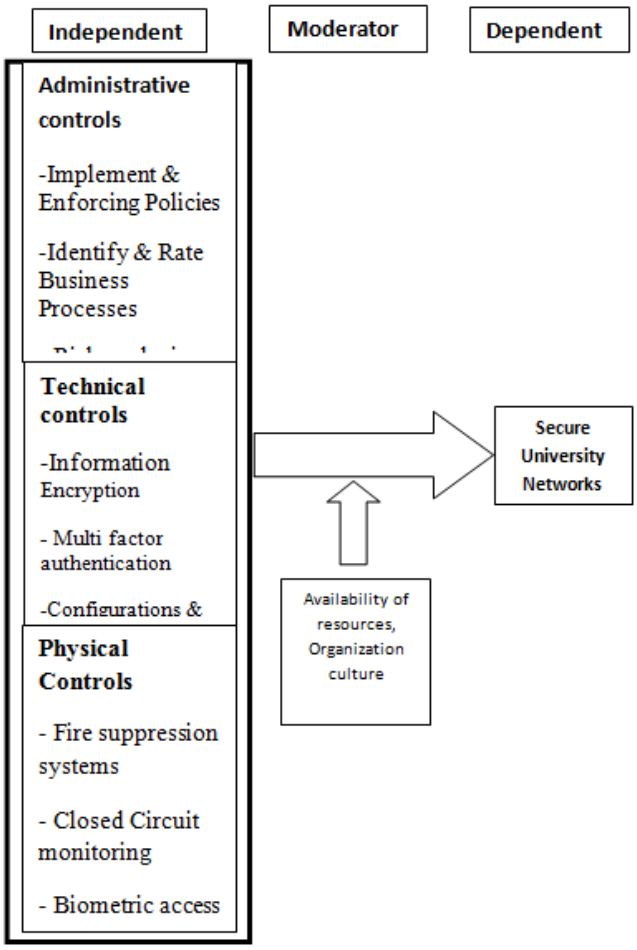

Figure 1: Conceptual Model

III. RESEARCH METHODOLOGY

This study utilized a cross-sectional descriptive survey with quantitative methods as it is useful at investigating and providing an in-depth insight into analyzing information security attributes that are used to secure university networks. The population of the study was 39 fully chartered universities in the country (Commission of University Education, 2017).

Further, the study employed probability sampling design which provided each university with equal chance of being included in the sample, (Kothari, 2004). The sample of study was determined by use of normal approximation to the hyper geometric distribution (Morris, E, 2004) as shown in the equation below:

$$n = \frac{NZ^2pq}{E^2(N-1)+Z^2pq}$$

Calculating sample size for small populations adopted from (Morris, E., 2004)

n = required sample size

N = population size

p and q = populations proportions value set for 0.5

E = Accuracy of sample proportions. Note for the sample proportions to be accurate E should not be lower than $^1/_n$ (Morris, 2004). Therefore, a value of {0.03} was used.

(Saunders et al, 2009), notes most business and management researches, researcher's use 95% of to within plus or minus 5% of the true value of 1.96 when using 95% confidence. Using the above equation, the sample size of the research study was found to be 38 as shown below:

$$n = \frac{39 \times 1.96^2 \times 1.5 \times 0.5}{0.03^2(39-1) + 1.96^2 \times 0.5 \times 0.5}$$

An application research randomizer was utilized. The universities were coded each with unique markers of p1 to p39 by the system for randomization; the institution that got the p39 value was dropped, one respondent was then chosen from each sample.

Purposive sampling was used to select respondents in the selected sample size; this was used because specific staffs are knowledgeable on the institution's information security status. Self administered close-ended structured questionnaire were used. This was guided by the vast nature of the data that was to be collected, the time available and the objectives of the study. Data collection instrument was pretested to determine their validity and reliability. The questions were formulated by the researcher and tested to ensure conformity.

Construct and content validity were utilized in the study. For construct validity a pilot study was carried out at the researcher's university's three different campuses to analyze and ensure the consistency of the respondents. For content validity guidance was sought from the supervisors and other experts from the School of Informatics and Innovative Systems in Jaramogi Oginga Odinga University of Science and Technology to establish it contains all possible items that were to be used in measuring the concepts.

The test-retest was administered to respondents of the university in the pilot study and the same test was also administered after 2 weeks. The scores from time 1 and time 2 were then correlated in order to evaluate the test for stability of time. To measure the degree to which the questionnaires yield consistent result or data, the researcher computed the Cronbach's coefficient Alpha technique to establish how items correlate amongst themselves to determine reliability. Evaluation of the framework was done using correlation and regression analyses and this confirmed the suggested relationships between variables in the framework.

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N
.790	.735	39

Table 2: Cronbach's alpha

This meant all constructs were internally consistent and measured the same content of the construct. The findings thus show that the questionnaire used in the study was reliable and the results of the questionnaire can be relied on as the alpha values were above 0.70.

IV. RESULTS

Descriptive statistical method analysis was applied to measure and determine the relationship that exists among the collected data. Objectives were analyzed using mean and standard deviation. The data was then analyzed descriptively with the mean and mode usage to understand and interpret variables. These allowed the analysis and presentation of large amount of data to be collected in the field. The study used regression model to determine the relationship between the dependant and the independent variables. The Pearson product moment coefficient (R) was used to establish the association between the independent and dependent variables based on the population data.

A. SECURITY STATUS IN UNIVERSITIES

Administrative controls respondents were asked about the existence of information security policies in their institutions 75% agreed information security policies exist in line with ICTA 2016, which sets standards for Government Enterprise Networks (GEN), which encompasses public universities as well. 2% were of respondents were not aware as to whether information security policies existed in their institutions while 19.44% indicated that information security policies did not exist.

66.67% of respondents acknowledged enforcement of information security policies which is in line with GoK vision 2030 in transforming connectivity and transmission, while 5.56% were neutral with no idea of what or whether there was enforcement of information security policies. 33.33% of respondents strongly disagree on having institutional critical business processes being distributed on the institutional infrastructure, 8.33% are oblivious as to whether there is any sort of distribution of processes or services.

Security threats to institution networks and systems can emanate from the use of counterfeit software, 65.79% of respondents strongly disagree on existence and use of genuine proprietary software on their core systems in their respective institutions and with 15.79% of respondents admitting entire institutions run any form of genuine proprietary software, 28.94% of respondents noted that use of genuine proprietary software on core systems, with all sorts of security vulnerability on institutions systems, indicating a lot more needs to be done to secure universities.

On whether institutions provided security training for its technical personnel, 55.26% disagreed to having any form of training provided, 39.47% agreed on having received training from the university. In line with provision of training,

respondents were asked whether they poses the adequate skill level to tackle cyber security threats, a cumulative 63.16% disagree they have the skills to detect or halt a cyber-attack, 36.84% of respondents agreed they acquire the skills to manage a cyber-attack, with 13.16 % strongly agreeing to be able to handle any cyber threat that may occur.

On technical/logical controls in the institutions, the question of multifactor authentication 21.6% of respondents agree on the use of multifactor authentication on their networks, 53.1% of respondents disagree on the use of multifactor authentication on their networks, this is of concern as the study confirmed social engineering as one of the major threats to universities,

Respondents were asked on the implementation of IDS/IPS systems, a cumulative total of 39.5% agree on the use of Intrusion Detection and/or Prevention systems which help in identifying threats attempting to gain access to the network. 50% of respondent disagreed on having IDS or IPS systems in place, this extremely dangerous as a malicious threat actor may hijack systems or have advanced persistent threats can have access to the network and the technical staff would not be aware of the threat. Only 15.7% of respondents agreed to audit and accountability of changes made to core systems on the network to keep track of any changes that would affect business continuity in the event of a catastrophic failure. 79% disagree on any form of auditing or accountability to changes made to core systems on the network this is of concern as a threat actor may make changes to core system configurations and the technical staff managing the systems would be none the wiser. Use of genuine proprietary software on the core systems used in the institution was queried an alarming 28.9% of respondents agreed to using genuine software and 65.8% disagreed on using genuine software on their core systems, this is extremely dangerous as output of counterfeit software cannot be trusted which can create financial risks to the institution.

Physical controls are best implemented by respondents from institutions, 81.6% of respondents agreed on access restrictions to the telecommunication room in the institutions indicating implementation of this physical control is well implemented in the institutions. 47.4% of respondents acknowledged the existence of power failure change over systems, this is still below average and more need to be done on this physical security control. 28.9% of respondents agreed to have CCTV surveillance in and around their telecommunications rooms.

B. SECURITY ATTRIBUTES

	Secure Network	Phys Ctrls	Tech Ctrls	Admin Ctrls	Org Culture
Secure Networks	1	.033*	-.059**	.206**	.054
Physical Controls	-.033*	1	-.139	.378*	.078
Technical Controls	-.059**	-.139	1	-.092	-.152
Admin Controls	.206**	.378*	-.092	1	.179
Organization Culture	.054	.078	-.152	.179	1

Table 3: Correlation analysis

ADMINISTRATIVE CONTROLS

The correlation coefficient of Secure University Networks and administrative controls is 0.206** indicating it has a positive correlation, with responses form a sample size 38 respondents and a p value of 0.000 from the 38 respondents, indicating a strong positive relationship between the two variables.

TECHNICAL CONTROLS

The correlation between Secure University Networks and Technical Controls is a positive correlation of 0.059**. Indicating the null hypothesis is rejected and the conclusion is there for a significant positive linear relationship between Secure University Networks and Technical Controls.

PHYSICAL CONTROLS

The correlation coefficient between physical controls and Secure University Networks is .033** with a p value of 0.001 from the 38 respondents, concluding that there is a significant positive linear relationship between the implementation of Physical Controls and Secure University Networks. The sig value is 0.001 indicating that there is a statistically significant correlation.

Step	-2 Log likelihood	Cox & Snell R Square	Nagelkerke R Square
1	.000[a]	.621	1.000

Table 4: Model summary table

Table 4: indicates that 62.1% of the outcome is predicted by the predictor variables. The model accounts for a significant amount of variation. This means secure university networks can be predicted significantly by how much physical, technical and administrative information security controls have been implemented.

	B	S.E.	Wald	Df	Sig.	Exp(B)
Z-Phys	2.310	1.022	4.263	1	.000	8.246
Z-Tech	-.341	.995	.054	1	.003	.794
Z-Admin	-.334	1.142	2.050	1	.002	.195
Constant	-.584	3.845	.010	1	.000	.681

Table 5: Variables in the Equation of security attributes

Physical controls significant value is 0.000, technical=0.003 and administrative is 0.002 this means that the correlation test for Secure Networks and physical, technical and administrative controls have a significant relationship, once the other variables are controlled for, there is a strong enough relationship between each of the variables to secure university networks. To interpret the differences between effects of respective secure networks controls to the predicted variable, the exp (B) column which represents the odd ratios for the individual variables is used.

Physical controls are 8.246 times more likely to secure university networks, technical controls are 0.794 times while administrative controls are 0.195 more likely to secure university network. This table generally gives the magnitude of the effects of the predictor variables are to have on the outcome of the dependent variable. In the model, the B values for each variable are also considered.

C. VALIDATED FRAMEWORK FOR UNIVERSITY NETWORKS

The result of the study is a secure framework for university networks which included all the variables in the conceptual model tested using regression analysis to identify if they have a significant impact on the security of university networks. The validated framework (Figure 3) emphasizes on the utilization of user involvement in order to determine the organizational goals and objectives.

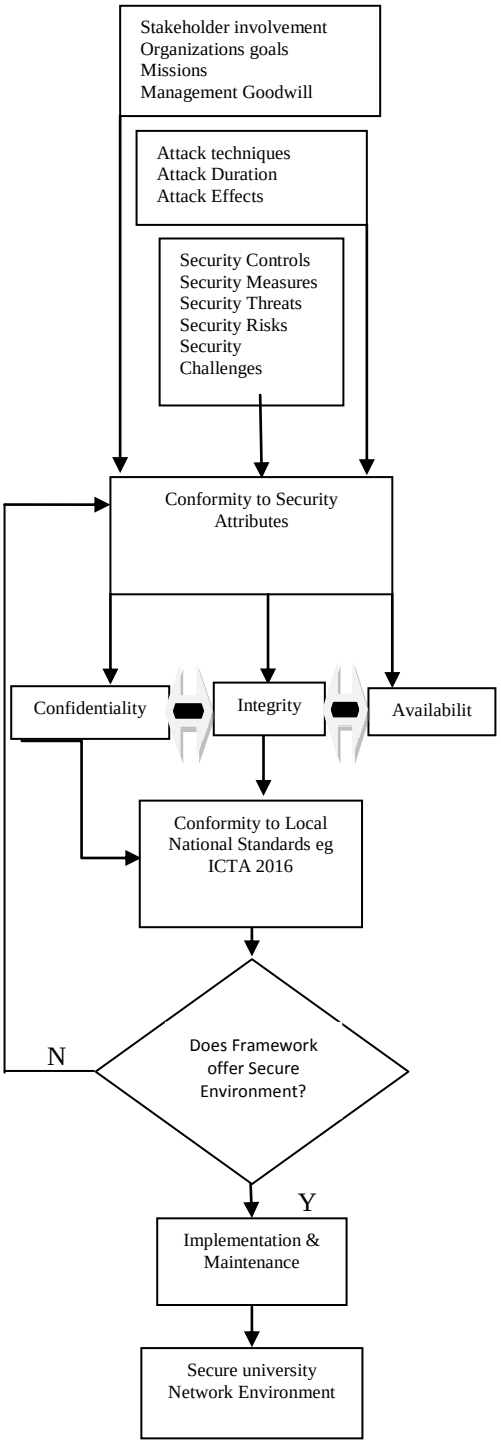

Figure 2: Frameworks for Secure Networks

V. DISCUSSIONS

Several factors were used and considered in establishing security threats to university networks; responses worth noting include core servers running counterfeit proprietary operating systems 65.79% of respondents concur to running counterfeit operating systems, similarly a question posed on end users running genuine proprietary with a paltry 13.2% of respondents running genuine operating systems on 100% of their networks. This is of concern as likelihood of malware attacks goes up exponentially, with risk of hijacking the network resources and using them to commit cyber crime. Auditing and accounting is also not carried out by 78.94% of respondents, this coupled the high figures of counterfeit software means administrators would not even be aware if a security misconfiguration or configurations changes by a threat actor, would not be known until it was too late. 55.3% of respondents not getting any form of cyber security training and 50% of respondents do not even caring out impact analysis on cyber resources in their institution and 55.26% disagreed on caring out any form of risk analysis, this coupled with counterfeit software running is a ticking time bomb for a large scale coordinated attack to university networks. The surprising fact is 78.9% of respondents agree on existence of security policies, with 92.1% of respondents agree on data sharing policies, indicating institutions are more concerned with data sharing and less about security. Cyber security seems acceptable on paper but actual implementation is barely carried out.

86.6% of respondents disagree on university technical staff being paid not commensurate with the industry standard which could be a potential security risk, this is an aspect that requires proper consideration since if the personnel meant to enforce security are the ones who break it because their financial status has been ignored and they are trying to make some extra money by circumvent security measures or doing "just enough" commensurate to their pay.

VI. CONCLUSION

The study revealed 95% of institutions allowed the use of personal devices (BYOD) on their campuses; this with a limited security foot print in implementation of cyber security measures is of concern. The countless BYOD devices create security concerns as multiple points of entry into the university networks are create, with the limited implementation of security policies and poor training of end users, its merely a matter of time till a cyber attack creates irreversible damage institutional data and reputation. The security controls respondents indicated a majority technical and physical security were well represented in their institution, but a large gap was seen in administrative controls indicating more work needs to be done by stakeholders of universities to ensure administrative controls stop being the bottleneck in securing institutions.

User knowledge on user domain knowledge and security policies and frameworks is basic, due lack of training and awareness, most policies are implemented in institutions as a legal requirement but not because of the benefit it provides.

VII. RECOMMENDATIONS

Institutions need to take the awareness and sensitization approach of technical personnel, staff and students seriously. From the study its alarming the casual nature at which cyber-security is taken. Security controls and more security measure need to be put in place especially with good will from university management teams. Further research need to be done on resistance of university teams in implementing administrative controls, also on creating a security policy that would be tailor made to fit in university unique data sharing environment and incredibly large BYOD gadgets in use on their networks.

REFERENCES

[1] Abomhara, M. (2015). Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks. Journal of Cyber Security and Mobility, 4(1), 65-88.
[2] Alkhamis E, Renaud K. (2016). The design and evaluation of an interactive social engineering training programme. In: Clarke NL, Furnell S, eds. Tenth International Symposium on Human Aspects of Information Security & Assurance, HAISA 2016, Frankfurt, Germany, July 19-21, 2016, Proceedings. Frankfurt, Germany: University of Plymouth; 125-134. http://www.cscan.org/openaccess/?paperid=282. Accessed May 23, 2019.
[3] Arana, M. (2017) How much does a cyber-attack cost companies? Open Data Security 2017, 1–4.
[4] Bayern, M. (2018, September 11). Why higher education is one of the worst industries at handling cyberattacks. Retrieved from https://www.techrepublic.com/article/why-higher-education-is-one-of-the-worst-industries-at-handling-cyberattacks/
[5] Breda, F., Barbosa, H., Morais, T. (2017) Social engineering and cyber security. In Proceedings of the International Conference on Technology, Education and Development, Valencia, Spain, 6–8 March 2017
[6] Cerullo, V., & Cerullo, M. J. (2004). Business Continuity Planning: A Comprehensive Approach. Information Systems Management, 21(3), 70–78. https://doi.org/10.1201/1078/44432.21.3.20040601/82480.11
[7] Chargo, M. (2018) You've been hacked: How to better incentivize corporations to protect consumers' data. Trans. Tenn. J. Bus. Law 2018, 20, 115–143.
[8] Costantino, G., La Marra, A., Martinelli, F., Matteucci, I. (2018) CANDY: A social engineering attack to leak information from infotainment system. In Proceedings of the IEEE Vehicular Technology Conference, Porto, Portugal, 3–6 June 2018; pp. 1–5.
[9] Coughlan, S. (2018, September 14). Students blamed for university and college cyber-attacks. Retrieved April 10, 2019, from https://www.bbc.com/news/education-45496714
[10] Elmrabi, N., Yang, S.-H., & Yang, L. (2015). Insider threats in information security categories and approaches [Research]. ResearchGate. https://www.researchgate.net/publication/283503171_Insider_threats_in_information_security_categories_and_approaches
[11] Farooq, M. U., Waseem, M., Khairi, A., & Mazhar, S. (2015). A critical analysis on the security concerns of internet of things (IoT). International Journal of Computer Applications, 111(7).
[12] Greer, C., Wollman, D. A., Prochaska, D. E., Boynton, P. A., Mazer, J. A., Nguyen, C. T., ... & Pillitteri, V. Y. (2014). Nist framework and roadmap for smart grid interoperability standards, release 3.0 (No. Special Publication (NIST SP)-1108r3).
[13] Jarrell, C., Dennis, R., Jackson, M., & Kenney, C. A. (2008). Academic and Student Affairs Issues Post Hurricane Katrina. Community College Journal of Research and Practice, 32(3), 235–250. https://doi.org/10.1080/10668920701875933
[14] Libicki, M. (2018) Could the issue of DPRK hacking benefit from benign neglect? Georg. J. Int. Aff. 2018, 19, 83–89.
[15] Li, S., Yun, X., Hao, Z., Cui, X., & Wang, Y. (2011). A Propagation Model for Social Engineering Botnets in Social Networks. 2011 12th International Conference on Parallel and Distributed Computing, Applications and Technologies, 423–426. https://doi.org/10.1109/PDCAT.2011.8
[16] Mitroff, I. I., Diamond, M. A., & Alpaslan, M. C. (2006). How prepared are America's colleges and universities for major crises?. Change: The Magazine of Higher Learning, 38(1), 61-67
[17] Mosenia, A., & Jha, N. K. (2016). A comprehensive study of security of internet-of-things. IEEE Transactions on Emerging Topics in Computing, 5(4), 586-602.
[18] Munyendo, B., Kimani, K., Kiio, G., Rishad, N., Ndung'u, M., Muema, M., Mwangi, A., & Ndung'u, M. (2017). SERIANU: Kenya Cyber Report 2017 (Annual 5th Edition; Kenya Cyber Report 2017, p. 80). Serianu Limited.
[19] Ounza, J. E., Liyala, S., & Ogara, S. (january 2018). International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064Index Copernicus Value (2016):79.57 | Impact Factor (2015): 6.391Volume 7 Issue 1, January 2018www.ijsr.netLicensed Under Creative Commons Attribution
[20] Pavkovi´c, N., Perkov, L. (2011) Social Engineering Toolkit—A systematic approach to social engineering. In Proceedings of the 34th IEEE International Convention MIPRO, Opatija, Croatia, 23–27 May 2011; pp. 1485–1489.
[21] Sabouni S, Cullen A, Armitage L, (2017). A preliminary radicalisation framework based on social engineering techniques. 2017 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA). London, UK: IEEE; 19-20.
[22] Symantec. (2015, April). Attackers Are Moving Faster, Defenses Are Not. Internet Security threat Report, 20, 5-6.Turner, R. (2018, March) 26). Social engineering attacks on the rise in higher education. UW–Madison Information Technology.
[23] Xiangyu, L., Qiuyang, L., Chandel, S. (2017) Social engineering and Insider threats. In Proceedings of the

International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery, Nanjing, China, 12–14 October 2017; pp. 25–34

[24] Segovia, L., Torres, F., Rosillo, M., Tapia, E., Albarado, F., Saltos, (2017) Social engineering as an attack vector for ransomware. In Proceedings of the Conference on Electrical Engineering and Information Communication Technology, Pucon, Chile, 18–20 October 2017; pp. 1–6.