IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Network Security Implementation: A case of Public and Private Universities in Kenya.

Dr. Charles Ochieng' Oguk
Mr. Francis Onyango

School Of Science, Technology And Engineering (SSTE)

Department of Mathematics, Statistics and Computing

Rongo University – Kenya.

ABSTRACT

While many scholars emphasize the importance of IT security management, existing studies hardly delve into the implementation of computer network security in institutions of higher learning. This study was conducted in the context of universities in Kenya, where it aimed at investigating the levels of implementation of IT security network's key performance indicators -KPIs. Questionnaires were as data collecting tools from university staff members. Collected data were analyzed to yield frequencies that were expressed in percentages and presented in tabular format. Results showed that while network security is vital for system security management, many universities have not adequately implemented vital aspects of network security. Further, in some universities where security appliances have been adopted, network penetration testing has never been done: and WIFI access is available through single universal password for any user. Therefore, it is recommended that network security's KPIs ought to be adopted in all universities to ensure improved information systems security management.

Keywords: network security, information systems security, user-group, ICT security.

INTRODUCTION

Anderson (2001) defines network security as the practice of establishing, implementing and maintaining the safety of information asset within inter-connected computing nodes of an organization, to safeguard confidentiality, integrity and full-time availability of the computing resources that it supports. According to Mang'ira and Kitoi (2011), fast computer networks have made the universities' data to remain accessible and sharable faster and more widely than ever before. Daya (2013) show that network is the main component of a robust automated computing systems upon which all the major automation tools for the university reside, and without which, any levels of automation may not be achievable.

In recent cases, compromised network security has been reported in many universities, where this results into data loss and breach of confidentiality. Consequently, critical data in the universities - mainly academic data and financial data have been faced with the loss and compromised confidentiality. Sekeres and Bevans(2016) noted that a hacker broke into the computer system of a university based in California that held financial data of over 80,000 stakeholders, causing unknown damages. Even though the damage was not immediately quantified, data confidentially, which is a core aspect of information security was nonetheless compromised. In Australia, IT students were found guilty of fraud and convicted for hacking and benefitting fraudulently from transport and bus ticketing system, (Bevans 2016).

In Africa, universities have experienced breaches of information technology systems to various levels. Jaffer, Ng'ambi and Czerniewicz (2007) noted that e-learning platform systems which are attached to university websites are mostly rendered unavailable whenever the university websites are attacked. Nweze (2010) showed that security breaches for computerized systems used in managing academics and administrative functions account for loss of investment in information systems in the universities in Nigeria. In 2015, a Ugandan university was attacked and security of the information systems breached. According to (Tibenderana & Ogao 2008), A university based Nairobi experiences close to a million attempted attacks daily by the new generation of hackers who trade on secret codes – bit coins, (Makori 2013). Similar online attacks occur in many organizations; but which mainly are never adequately reported, (Makori & Oenga, 2015).

However, there is need to review the functional components of a robust network structure to counter these attacks, (Oguk, 2016). According to Mullard (2007), network security at the elementary levels include; hierarchically managed network design, secured network with virtual segmentations e.g. VLANs, regular penetration testing against network, internet bandwidth management tools, alternative internet service provision, and the existence of redundant back-bones. But since a compromised network security implies that all the resources including data, the host computer as well as all the applications remain vulnerable to security breaches, (Peterson & Davie, 2007), it is paramount to shed light into the levels of implementation of the these components of network security in the universities.

Statement of the Problem

Globally and here in Kenya, universities experience compromised network security which affect confidentiality, integrity and availability of the resources therein. Despite this, related studies have hardly focused on the adoption of the key components of network security within the universities, - the main focus of this study.

Objective

The main aim of this study was to investigate the levels of implementation of the key components of network security in universities in Kenya.

REVIEW OF RELATED STUDIES

While studying network security among the US-based universities, Daya (2013) defined computer network security as an IT security approach consisting of the practices and policies adopted to control, prevent and monitor unauthorized access, modification, misuse, or denial of a services in an interconnected computer based resources.

Globally, weak network security has been attributed to breaches of information systems in a member of universities. In the year 2016, for instance, VMware group explored the evolving cyber threat within UK universities and how the institutions can be safeguarded against cyber-attacks. The study revealed that there is a very high likelihood of the universities being attached due to vulnerabilities in their networks Tzu-Chin (2016). Tzu-Chin showed that 79 percent of the UK universities have experienced damage to reputation due to cyber-attack, whereby 74 percent of those attacked were forced to halt vital research projects due to research data losses associated with cyber related attacks on their computer networks.

According to the study by Daya, a stable and secure IT infrastructure confidently supports organization's core business and also provides safe computing environment. While showing agreement with this, Mullard (2007) further showed that secure computer network increases accessibility of resources to authorized entities, data integrity, data authentication, non-repudiation, confidentiality, privacy and availability. As such, Mullard explained that network security at the elementary levels include network data security, network access control and monitoring, network malware control and network security policy. This view was also held by Broadbent (2007), which argued that security policies around external and internal access control within data networks in Germany could constitute sound strategy for information security management. Peterson and Davie (2007) nonetheless, suggested that people, mainly the systems' users should be considered under policy issues. Peterson and Davie also showed that a compromised network security implies that all the resources including data, the host computer, people and all the applications remain vulnerable to security breaches.

Further, Daya (2013) claimed that IT infrastructure supported by insecure network hardly supports organizations' business objectives, since it is vulnerable to attack. In the research, Daya identified increased accessibility of resources to authorized entities, data confidentiality, system authentication, data integrity, non-repudiation, availability and privacy as the most important objectives of secure computer network. Also, Mullard (2007) showed that to ensure network security, there should be regular vulnerability assessment, resource availability, access control,

user management, security policy, software patches/updates, malware control, data security controls, and proxy-management. Similar findings emerged in a study by Martins, Eloff, and Park (2001) which asserted the need for network hierarchical structure, virtual network segmentations, regular penetration testing, internet bandwidth management tools, alternative internet service provider, and redundant back-bones in the Local Area Network – LAN, and network security policy as the features of computer network security.

Stressing the role played by computer network in university in South Africa, Jaffer, Ng'ambi, and Czerniewicz (2007) demonstrated that both voice and data communications ride on computer networks, and support workflow through automation tools like ERP in the university. The use of sub-elements of network security in management of information systems' security is further supported by Deloitte Kenya (2011), which conducted a similar study within East Africa. Deloitte, however, suggested the incorporation of people, especially the systems' users, to be considered along the features of network security as mentioned earlier. It showed that network security should be addressed much effectively to ensure safety of the entire information asset.

Considering the importance of network security to the entire information systems in universities, Eira and Rodrigues (2009) indicated that even system hackers have to break the network defense first, before accessing the host computer bearing the application systems in order to reach the applications and the data. Eira and Rodrigues thus demonstrated that where there is effective network security, data security could be improved by making the data more difficult to reach by hackers. This view was however, opposed partially by Okibo and Ochiche (2014), which demonstrated that high internet bandwidths in a university computer network has been exploited by system hackers to reach the host computer and finally compromise data security in the host computer.

Makori (2013) studied network security management within universities in Kenya and showed that local computer networks are supplied with high internet bandwidths that facilitate online access to information resources, not only by the stakeholders, but also expose the entire university computer resources to the insecure world through the internet. Makori claimed that the high bandwidth facilitates unauthorized access to the universities' information asset, thus exposing information systems to risk of compromise. This view is supported by Mulwa (2012), which showed that, the sensitive data residing in the Kenyan universities' computer networks attracts hackers from both inside and outside the university, who try to access the information and its assets in order to manipulate the information for their selfish gain. Both Mulwa and Makori portrayed network security as a very important aspect of IT security, and separately argued that it should be considered in an IT security management program. On the contrary, Arora (2010) stressed that despite high internet bandwidths, when effective network security management tools are implemented properly, network layer would still offer protection to data and underling applications.

In summary, in the studies highlighted above, network security is viewed as an IT security approach consisting of the practices and policies adopted to control, prevent and monitor unauthorized access and facilitate appropriate utilization of resources within interconnected computer systems within a uneasily. They highlighted key features of network security as: hierarchical network design; secured network with virtual segmentations e.g. Virtual Local Area Networks - VLANs and user groups; regular penetration testing against network; internet bandwidth management tools; alternative internet service provision, and the existence of redundant back-bones among other features.

The gap

However, despite the cases of compromised security of university computer networks, the level of implementation of the key features of network security in organizations have not received much attention. It is against this view that the extent of implementation of network security features in universities needed to be investigated.

RESEARCH METHOD

The following research methodology was employed.

Research Design

The exploratory research design was adopted in this study due to the necessity of a firsthand understanding of the levels of implementation of network security measures employed to secure university information systems in Kenya. This approach was informed by the realization that the study spectrum is relatively recent and inadequate research work is documented on this topic.

Population

The target population for this research included the sectional leaders of 13 computing sections (as supported by scholarly studies) in seventy (70) universities in Kenya according to CUE in the year 2015. Therefore a population of (13x70= 910) section leaders in the universities.

Sampling

The multiple sapling approach was employed, stratified sampling was used to categorize universities into public and private universities. Random sampling at ten percent (backed by studies) was employed on the two strata separately to yield a total of seven (7) universities where the study was conducted. See table below.

The university population and the sample

	Stratified Sampling	Simple-Random Sampling
Public universities	33	3
Private universities	37	4
Total	70	7

Finally, purposive sampling approach was applied since the category university staff who are rich in the required data was known: mainly the ICT staff members and heads of the various sections heads of user departments. See table below.

Purposive Sample sampling

Operation Area (Category)	No of team leader(s)	Sample size	Totals
IT leadership	1		
System 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 Laboratory	1	7	7
Students Leadership	1	7	7
Totals	**13**		**91**

Data collection instruments, direct observations and well designed questionnaires were used for data collection

Data analysis and interpretation

In this study, both qualitative and quantitative analyses were employed. Data was analyzed using SPSS software and Microsoft Excel to yield pertinent statistical values addressing the objective of the study. With regards to qualitative data analysis, respondents' views on implementation levels of network security safeguards were rated as based on their effectiveness. With reference to quantitative approach, frequency-based percentage levels of implementing the network security safeguards were presented mainly in tabular format.

RESULTS

Demographics of the respondents were summarized as shown in the table below, where close to 40 percent were ICT staff members and others representatives of various user departments.

Area of the university

Operation Area	Percentage
ICT staff	39.4
Finance	11.3
Admissions	7.0
Examinations	8.5
Human resources	9.9
Audit	4.2
Library	9.9
Health centre	8.5
Computer lab	1.4
Total	**100.0**

Total internet bandwidth levels in the university

Internet Bandwidth levels (Mbps)	Percentage
Above 100	60.0
61-100	8.0
30-60	16.0
Below 30	16.0
Total	**100.0**

This study found that there is high internet bandwidth supply within the universities with more than 60 Percent of the universities subscribing to above 100 Mbps internet bandwidth. Most universities have secondary internet service providers (ISPs) which are 36 percent effective. This finding concurs with Mang'ira and Kitoi (2011) & Makori (2013), which fast computer networks have made the universities' data to remain accessible and sharable faster and more widely than before. This situation exposes the entire university computing resources to the insecure world through the internet.

While this finding agrees with the two independent studies above, it further shows that most universities have secondary internet suppliers. Some ISPs like KENET allow more than double of the amount of internet subscribed in the evenings, throughout the nights and all over weekends at no additional cost. Due to the high internet supply levels, the universities remain prone to attacks from outside as the external attackers do rely mostly on the fast

internet to launch attacks. The study also revealed that all the institutions under survey have adopted firewalls to provide network security at the server levels.

In addition, the study found that 56 percent of the local area networks in the universities are not hierarchical but flat, thus making it difficult to effectively manage them. 52 percent of the university networks are still not segmented, meaning users can still access resources freely from any part of the network, without restrictions. For universities with security appliances, 72 percent have not effectively conducted penetration testing, thus are not aware of the effectiveness of the security appliances employed. 56 percent of the universities do not have effective tools for internet bandwidth management. If the entire internet bandwidth drop in a university's local area network cannot be managed, it could be a sign of misused bandwidth resource and high level vulnerable to attack, (Oguk, 2016).

The current study further revealed that up to 76 percent of the university networks do not have redundant core back-bones. Redundant back-bones help to reach given access networks in case the primary back bone is down, to ensure continuous systems availability. This was suggested as a remedy for system back-up problems by (Ismail & Zainab, 2011). 60 percent of the universities do not effectively control access from external networks while only 32 percent are controlling the access from internal threats effectively. 60 percent of the respondents do not effectively implement web-content filtration, meaning access to any universal resource locators (URLs) is not restricted in such universities. This is a security threat as this uncontrolled access may encourage social engineering and spam injection into the university information systems.

The problem of un-managed university network is further shown in the study by the revelation that 56 percent of the universities have not effectively configured the active directories. In some universities, windows server operating systems exist, yet the security features like active directories have never been activated. Over 82 percent of the universities have well controlled user groups with members restricted to given access privileges. Besides, access to given internet sites from the university local area network is restricted in over 75 percent of the universities.

Most of the universities have improper controls for wireless resources like access to the university WIFI, whereby only 44 percent of the users therein use unique user account and a corresponding unique password for every user. 56 percent of the universities however, apply one common and universal password for all and any users within the universities to access the WIFI.

In order to improve security of systems within network infrastructure, various measures are adopted. For instance, the use of IT security training programs, threat awareness program for both system's users and administrators, well configured firewalls, implementation of intruder detection and prevention systems, honey-pots, De-Militarized zones, Unified Threats Management, User-groups, system controlled password expiry, user authentication mechanisms like:

bio-Metrics, access control cards and any similar combinations with passwords. The approaches help to minimize security incidents within the high bandwidth internet connection, (Mallard 2007).

Availability of network security features

	Response (percentage)	
	Yes	**No**
Intruder detection / prevention system	56	44
Honey pots and De-Militarized zones	68	32
Firewall	100	0
Unified Threats Management System	44	56
controlled User-groups	24	76

An intrusion detection and prevention system (IDPS) is a security appliance, which can be a hardware or software that monitors a network for suspicious and malicious activities as well as policy violations, detects the activities and prevents them. The IDPS system then reports any detected violation of policy with to an I.T. Administrator. Bulgurcu, Cavusoglu and Benbasat, (2010) showed that while (IDPS) have been used in most universities across the world to beef up security, some institutions still do not consider them as important remedies for network security. It further showed that user-groups, honey pots and De-Militarized zones are complementary security appliances that enhance network security. The study showed that while 56 percent of the respondents do not use (IDPS), only 44 percent of the respondents apply them. Further, only 32 percent of the institutions sampled use Honey pots and De-Militarized zones in their entire information systems infrastructure.

The application of User groups in system security management

User groups are very important in information systems' security management as it outlines the boundaries of access to the computer resources, accords different access privileges and also separates systems users from administrators. According to Mohlabeng, Mokwena and Osunmakinde (2012), users-groups are important in the general IT infrastructure security management within South-African institutions of higher learning. Also, Nyamongo, (2012) and Jansen, (2010) show that holistic information systems' security framework including user-groups can offer better security management for IT systems in universities.

It this study, it was found that 76 percent of the respondents indicated the availability of user-groups within the universities, results which are consistent with both Nyamongo (2012) and Jansen, (2010) findings. Unified threat

management systems (UTM) is a systems' security appliance that handles mltiple security features at the same time, for example PRGT, Mikrotik, and Cyberoam systems. They are important in automating security administration for information systems. Also, 56 percent of the respondents confirmed UTM presence in their universities, while 44 percent do not.

DISCUSSION

This study found network security elements as being useful in the management of IT security within the universities in Kenya. With this regard, it was found that there is high internet bandwidth supply within the universities. In addition, the study found that 56 percent of the local area networks in the universities are not hierarchical but flat, thus making it difficult to effectively manage the network security. 52 percent of the university networks are still not segmented, meaning users can still access resources freely from various parts of the network, without effective control of users' resource allocation. For universities with security appliances, 72 percent have not effectively conducted penetration testing, implying that the effectiveness of such security appliances have not been put to test. The current study further revealed that up to 76 percent of the university networks do not have redundant core back-bones; hence poses a challenge of un-availability. Also, 56 percent of the respondents confirmed UTM presence in their universities, while 44 percent did not. However, 56 percent of the universities apply one common and universal password for all users within the universities to access the WIFI. This is a major security issue, as users on universal WIFI access passwords are not easily controlled or even trailed on the systems audit trails section.

The findings on adoption of network security in the universities agree with Anderson (2001) which showed that network security helps to safeguard confidentiality, integrity and full-time availability of the computing resources that it supports. Further, the findings are in agreement with (Ismail & Zainab, 2011; Makori & Oenga, 2015; Oguk, 2016 & Daya 2010), that although network security constitutes a vital part of IT security management in; there is inadequate implementation of network security controls making them vulnerable to compromises which again are not well reported. Further, the findings that 76 percent of the respondents indicated the availability of user-groups within the universities is consistent with both Nyamongo (2012) & Jansen, (2010) findings, which highlighted user-groups as effective for IT security management.

Summary, conclusion and Further Research

Results showed that while network security is vital for system security management, many universities have not adequately implemented the most vital feature of network security. In addition, in some universities where various network security appliances have been adopted, penetration testing has never been done - meaning the effectiveness of the appliances may not be estimated. Further, WIFI access remains available through single universal password for any user. This further makes the entire information systems vulnerable to access. Therefore, it is recommended that network security's KPIs should be adopted in all universities and database authentication be adopted of WIFI access to ensure improved information systems security management. A research should be conducted to determine the best freware network security management tools due to high cost of information systems security appliances.

REFERENCES

Arora, V. (2010). Comparing different information security standards: COBIT v s. ISO 27001. *Línea. Disponible en Carnegie Mellon University, Qatar:(http://qatar. cmu. edu/media/assets/CPUCIS2010-1. pdf)*.

Bichanga, O. W., & Obara, 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.

Bevans, B. (2016). Categorizing Blog Spam.

Broadbent, J. (2007). If you can't measure it, how can you manage it? Management and governance in higher educational institutions. *Public Money and Management*, *27*(3), 193-198.

Chi, S., Park, J., Jung, K., & Lee, J. (2001). Network security modeling and cyber attack simulation methodology. In Information Security and Privacy (pp. 320-333). Springer Berlin/Heidelberg.

Daya, . (2013). Network security: History, importance, and future. *University of Florida Department of Electrical and Computer Engineering*.

Deloitte, L. L. P. (2011). Mobile telephony and taxation in Kenya. *Nairobi: Deloitte LLP*.

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.

Jaffer, S., Ng'ambi, D., & Czerniewicz, L. (2007). The role of ICTs in higher education in South Africa: One strategy for addressing teaching and learning challenges. *International journal of Education and Development using ICT*, *3*(4).

Makori, A. C., & Oenga, L. (2015). A survey of Information Security Incident. *Computers & Security*.

https://doi.org/http://dx.doi.org/10.1016/j.cose.2014.11.006

Martins, A., Eloff, J. H. P., & Park, A. (2001). Measuring information security. In *Proceedings of Workshop on Information Security–System Rating and Ranking*.

Mingaine, L. (2013). Skill challenges in adoption and use of ICT in public secondary schools, Kenya. *International Journal of Humanities and Social Science*, *3*(13), 61-72.

Mang'ira, R., & Andrew, K. (2014). Towards establishment of a full-fledged disaster management department for Moi University libraries.

Mulwa, A. S. (2012). The influence of institutional and human factors on readiness to adopt E-Learning in Kenya: The case of secondary schools in Kitui district. *An unpublished PhD thesis of the University of Nairobi*.

Nweze, C. M. (2010). The use of ICT in Nigerian universities: A case study of Obafemi Awolowo University, Ile-Ife.

Nyamongo, D. M. (2012). *Information systems security management* (Doctoral dissertation, Strathmore University).

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.

Oguk, O. C. (2016). Review on Mobile Network Security Issues and Challenges. *Mara*.
Oguk, C., Karie, N., & Rabah, K. (2017). Network Security Management in Universities in Kenya. *Mara Research Journal of Computer Science & Security*, *2*(1), 48-60.

Pfleeger, S. L., & Cunningham, R. K. (2010). Why measuring security is hard. *IEEE Security & Privacy*, *4*(8), 46-54.

Sekeres, M. A., & Bolwell, B. J. (2016). Will cancer patients be the next victims of the data privacy debate. *FoxNews. com. Accessed April*, *19*.

Tzu-Chin. R. (2016). A Scale of University Students' Attitudes toward e-Learning on the Moodle System. *International Journal of Online Pedagogy and Course Design (IJOPCD)*, *4*(3), 49-65.

Zhu, J. (2015). *Optimization of power system operation* (Vol. 47). John Wiley & Sons.