INTERNATIONAL JOURNAL OF SOCIAL Sciences and Information Technology
ISSN 2412-0294 www.ijssit.com
http://www.ijssit.com

THE MAJOR ELEMENTS FOR INFORMATION TECHNOLOGY SECURITY MANAGEMENT IN UNIVERSITIES IN KENYA

[1*] **Oguk Charles Ochieng'**
ogukcharles@gmail.com
ogukcharles@rongovarsity.co.ke

[1] *Rongo University, Kenya*

Abstract

Despite continued investment in information technology security systems within universities in Kenya, there has been increased frequency of information systems' security breaches. Studies indicate that information technology security management could be enhanced by focusing resources on specific elements. However, continued breaches within the universities is attributed to haphazard investment on security controls without focus on specific elements. The objective of this study was to identify the major elements and investigate their application in management of information security within universities in Kenya. Secondary publications were reviewed to ascertain the major information technology security elements and questionnaire based survey conducted to seek the extent of application of the elements within the universities. 10% of universities was sampled randomly. Further, purposive sampling was used to collect data targeting IT personnel. Data was analysed using SPSS, where mean scores for the various elements' contents were expressed as percentage. In conclusion, while the level of implementation of major IT security elements contribute to better security management, most elements were not implemented to the levels of expectation. Therefore, it is recommended that more resources should be directed to the major elements for better information systems security management.

Keywords: *IT security, IT security elements, IT security management*

Introduction

IT security management refers to the practice of coordinating activities, regulations and operations that direct and control the preservation of confidentiality, integrity and availability -CIA of information asset, (Tipton & Krause, 2000). Mulwa (2012) noted the increased dependence on information technology by universities in Kenya, thus raising focus on IT security management. Also, Makori (2013) noted that there is increased dependence on Information Technology within universities in Kenya, where technology facilitates handling of academic and administrative data at the levels of file generation, storage, processing, caching, long haul transit and transfers through local area networks – which in effect expose the university's data to cybercriminals and other threats. Moreover, students, employees, criminals, contractors and visitors pose security challenges for university information safety. According to Tipton and Krause, information systems' security management practices in the universities concentrate on areas directed more by intuition rather than sound technical pillars of security. Therefore, there is a need to focus on the major elements of security infrastructure as effective measures for management of information systems security in universities. Luambano and Nawe (2004) found

that the major IT security elements revolve around data security, computer network security, security policy, physical security and access control.

In the year 2013, a university in US reported that two students faced charges for allegedly breaching the school's computer system security and created for themselves and 50 other student's better grades through recording keystrokes made by instructors as they logged into the system. Another university in Texas had student information system compromised by malicious hackers using brute force attack exposing more than 55,000 names, e-mail addresses and Social Security numbers of faculty members and students. The institutions' authorities admitted that the situation could have been avoided even through ordinary and basic proactive management tools. 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 be protected using effectively implemented IT security policy.

Many cases of physical security incidents affecting universities' information systems in Kenya are many, but which remain unreported. 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. Mang'ira and Andrew (2014), highlighted that availability of information systems' resources in Universities in Kenya is affected not only by hacker activities, but also by physical security incidents like natural disasters, accidental and deliberate actions including: disconnection of network cables, computer theft, vandalism, floods, sabotage, fire, strikes / riots and lighting. Whenever the physical security systems are breached, the incidents exposé information systems of the universities to high level risks of data loss and compromised content integrity.

Since the year 2012, for example, a public university in Kenya has experienced more than three incidents of both internal and external cuts on fiber- optics lines, which rendered the entire information systems unavailable for users. In 2014, inter-block fiber optics cable linking the university's server – room and office of the registrar- academics was accidentally cut by laborers when weeding along street flowers, which was traversed by optical fiber back-bone underneath. This incident made the university server that was hosting students' data to be unreachable, thus unavailable for the affected department for weeks. It was noted that there was no signage identifying areas traversed by data lines within the university. The university reportedly lost two desktops from the students' computer lab in the year 2013 as the loss was attributed to inadequate physical interventions. This was as well attributed to uncontrolled physical access to ICT premises.

In November 2015, another Kenyan public university's IT system was struck by lightning, compromising information system's availability. Makori (2013) indicated that insiders have breached system access controls for information systems in the universities thus gaining unpermitted access. In Kenya, physical access control in a university's computer laboratory was breached and at least two desktops went missing in the year 2013. Also, in another university in Kenya, students compromised access control of the student's management information systems' security in the year 2011. The rising incidents of compromised IT security systems in universities are associated with investment not focused on elements of IT security.

Statement of the problem

Information security is vital for safety of academic data resources in universities in Kenya. However, studies undertaken by Mong'ira 2011 among other studies showed that most IT security related investments within universities in Kenya hardly focus on major elements of IT security, thus leading to ineffective IT security management. As such, there is rising cases of compromised information systems in the universities despite continued investment in IT security.

Many studies exist on the instances of information security in university information systems, information protection approaches, cloud security, network security and security sensitization. However, scholars have made limited efforts by on exploring the major elements of information security for better management.

Purpose: the purpose for this study was to identify the elements of information systems' security and investigate the elements' levels of implementation within universities in Kenya.

Objectives

1. To identify the major elements of information systems' security within universities in Kenya.
2. To investigate the implementation levels of the major elements of formation systems within universities in Kenya.

Significance of the study

A research on information technology security management approach based on major IT security elements, had not received much academic focus within the universities in Kenya, prior to this stud. This study helped to highlight an IT security management approach that holistically considers major IT security elements including; security policies, network security, physical security, data security and access control as IT security management pillars within universities. Since the performance of every major IT security elements was considered in this approach, it may help universities' managements to concentrate resources on specific elements of IT security, thus facilitating prudent use of resources in improving the systems security.

Scope of the study.

The research was conducted to identify and investigate the application of major elements of IT security in managing IT security within universities in Kenya. This was conducted between the years 2017 and 2018 and mainly focused on the responses of IT security personnel and lead systems users.

Assumption of the study: the study assumed that all the universities in Kenya had adopted appreciable information systems in their various operations.

Literature Review

The Elements of information technology security

There are many information technology security elements, but which fall under broad areas of technology, processes and people. According to Casey (2011), information security elements emanating from the three broad categories of; technology, processes and people can be classified further into major and minor IT security elements. The study agreed with a review of Martins, Eloff and Park (2001) & Luambano and Nawe (2004) which showed the major elements of IT to include: security policies, physical security, network security, data security, and access control. Since the elements are highly useful contributors to IT security status, they should be explored further for IT security management within universities. This study, therefore, has analyzed

information on the levels of implementation of the elements of information technology security within the universities.

The major elements of IT security

According to Makori (2013), implementation of IT security along the major elements of information technology security directly facilitates secure operations for the universities' academic and administrative functions, which rely on automated information systems. On this note, Veseli (2011) demonstrated that the effective management of IT security appliances at the elementary levels helped executives in improving information systems security as well as quantifying returns on IT security investment among Norwegian University.

IT Security Policy

Bulgurcu, Cavusoglu and Benbasat (2010) reviewed that IT Security Policy is one of the most critical elements of an organizational IT security program. It 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. Siponen and Vance (2010) noted that physical access control, which involves perimeter walls, appropriate signage along network transmission media, secure computing premises are catered for in a well written information security policy. 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 policy remains a challenge that makes many institutional information systems' security to be easily compromised, (Huber, Flynn & Mansfield 2016). A study was conducted in universities in 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 control in IT security management. Jagadeeshwar, Shriramoju and Babu (2016) showed 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. 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 preceding studies reiterate that IT security policy is so important that it should be incorporated in development of information systems security management program. It has also 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 sub-elements should, therefore, be considered as the building blocks for IT security policy within an organization's IT security structure.

Physical security

According to Casey (2011), universities use both hardware and software computer facilities whose security levels in the surrounding environments should be considered. The facilities are kept safe in some forms of physical enclosure for security provision, for example, metallic grills, perimeter fences and locked server - rooms, (Stallings & Brown 2008). In many cases, Universities' information systems have been rendered unavailable by disconnected network cables, hardware theft, and system vandalism, (Pfleeger & Cunningham, 2010).

These experiences concur with Mitnick, and Simon, (2011), which reviewed information systems, and concluded that physical security is a crucial element worth considering when developing IT security management model. The study concluded that KPIs for physical security should include: implementation of signage to identify IT resources, implementations of physical barriers around physical IT systems assets, maintenance of IT asset register, access control to physical facilities hosting IT systems, and secure storage and monitoring of facilities for instance, through closed circuit camera television - CCTV.

The studies stress the need for incorporating physical security features in the development of IT security management program, to show the levels of physical interventions and practices adopted in an organization for IT security management. The highlighted KPIs constitute the building blocks for physical security as a major element of IT security in the management approach.

Network security

Anderson (2001) defined 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 before. Daya (2013) showed 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.

Both voice and data communication ride on computer networks, and support workflow through automation tools in the university, (Anderson, 2001). Eira and Rodrigues (2009) indicate that even system hackers have to break the network defense first before accessing the host computer bearing the application system. According

to Martins, Eloff, and Park (2001), wide area networks - the internet has been exploited by system hackers due to the increase bandwidth and weak security at the host side.

According to Daya (2013), a stable and secure IT infrastructure confidently supports organizations' core business and also provides safe computing environment. Mullard (2007) stressed the importance of secure computer network and showed that it; increases accessibility of resources to authorized entities, data integrity, data authentication, non-repudiation, confidentiality, privacy and availability. Arora (2010) thus asserted the need for considering network security as a key element of the entire information technology security. 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. The sub elements of network security elements are supported as KPIs in similar research studies like the one conducted by Deloitte Kenya (2011) within East Africa. A compromised network security implies that all the resources including data, the host computer and all the applications remain vulnerable to security breaches, (Peterson & Davie, 2007).

Data security

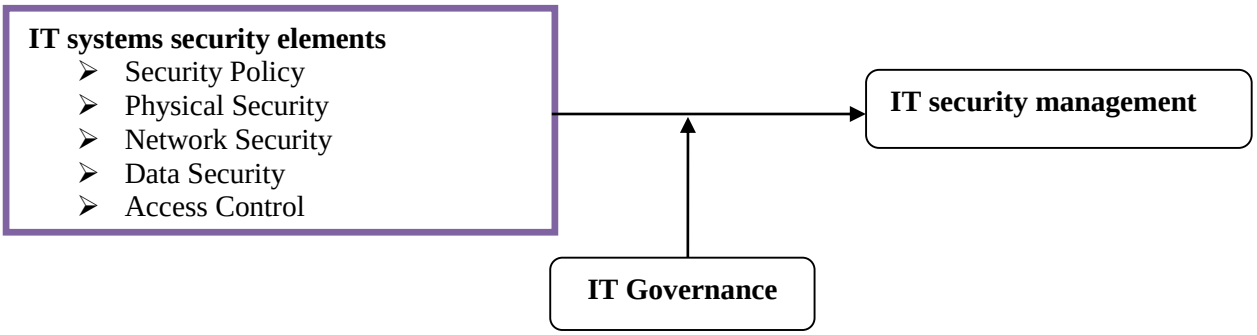
According to Selwyn (2007), the adoption of information systems and associated technologies has created a robust platform, associated with more efficiency in handling academic and administrative data at the levels of file storage, data generation, data processing, signal caching, long distance transit and transfers through internet. Automation systems supporting seamless student registration systems, financial transactions and examinations are used in the universities, hence they contribute the major sources of data (Ndung'u 2015). Enterprise resource planning system - ERP generates so much data in electronic form that reside in the university operating network. The network therefore, needs much controls to guarantee data integrity, Galliers, and Leidner (2014). Tarus, Gichoya and Muumbo (2015) e-learning has been adopted in the universities in Kenya to successfully reduce financial as well as geographical barriers to higher education. There is therefore a need to incorporate data security as a vital element in the management of information systems security in the universities.

Access control

Shelc (2015) defined access control as the limitation of entry into an information system only to authorized persons, in order to safeguard the confidentiality, integrity and availability of information systems. According to Mulwa (2012), the features of access control that constitute its building blocks are: control access from external networks, web content filtration, control of access form internal networks, well configured active directory and user-group boundaries. Luambano and Nawe (2004) noted information security concerns as student exam management systems, financial and payment systems in universities are mostly web-based and hence the data generated remain accessible not only through the internet, but also via mobile systems.

Regarding information systems security, Sridhar, & Govindarasu (2014) showed that data storage, use and transfer through computer networks expose the university's data to cyber-criminals and other threat agents, a view held as well by has (Oguk, Karie & Rabah 2017). Luambano and Nawe (2004) reviewed that data security is built up by features like; encryption of data files, users' restrictions to data resources, which are all attempts meant to control access. The studies underscored the importance of implementation of the features access control and the need to incorporate them in IT security management program. The foregoing discussions confirm that access control is so important to IT security management that its features ought to be included in the development of IT security management.

Conceptual framework



Source: Author, 2018

Methodology

Secondary publications were reviewed to ascertain the major information technology security elements and questionnaire based survey conducted to seek the extent of application of the elements within the universities. Ten percent of the universities was sampled randomly and further, purposive sampling was employed for data collection targeting IT personnel only. Data was analysed using SPSS, where the mean scores for the various elements' contents were calculated and expressed as percentage.

The approach employed for ascertaining the major IT security elements considered in the management of IT security was the adoption of well designed questionnaire. The target population for this research was 910 respondents resulting from the seventy (70) universities in Kenya according to CUE in the year 2015; Mukhwana, Kande and Too (2017). Team leaders of various categories of information system users and IT administrators formed the target for data collection. For the purposes of this study, ten percent (of 910 respondent from the 70 universities = 91 respondents) was sampled. The reliance on sample size equivalent to ten percent of a population to provide fair base for analysis is supported by (Mugenda & Mugenda, 1999); (Rubin & Babbie 2012) & (Kothari 2003). The 7 universities sample was constituted by samples under public and private university categories. Further, purposive sampling was used to obtain response from employees . Since not every staff member in the entire university work force deals with information systems whose work involved information systems. Consequently, users and administrators of IT systems were considered to be richer in information needed for the study, especially, in IT security experience and data desired by the researcher.

Moreover, data that was collected from IT departments was concerned with: IT leadership, network administration, systems administration, security administration and database administration. The categories above were preferred for this study for the purpose that employees therein directly interact with information systems in their day-to-day operations within the universities, and were thus potential victims of IT security breaches. Data was therefore collected from one respondent (the team leader) of each of the thirteen (13) operation areas in every university, including both IT personnel and the information systems' users. The data collected gave information mainly on: IT security policy, physical security, network security, data security and access control areas of IT security. Being that a sample of seven (seven universities) was considered for the study, the total sample size was (13 x 7 = 91 respondents). The primary data on information technology security elements collected through the questionnaire was subjected to descriptive statistics mainly the measures of central tendency - the mean, so as to reveal the average gap under investigation for the sub-elements within the main elements of IT security. The mean score for sub-elements was used as the average

security status levels for the given elemenent of information technology under consideration as based on the implementation levels.

Data Analysis, Compilation And Discussion Of Results

The objective sought to investigate the major elements of IT security and their application in management of IT security within universities in Kenya.

Ascertaining information technology security elements

Review of secondary information, especially the research work on information technology security was done to ascertain the key information technology security elements in chapter two above. The key security elements of information technology are very important, since the levels to which they are implemented, adopted and practiced within the universities can be used to determine the prevailing information technology security status at the elementary levels (Luambano & Nawe 2004). The major elements, according to the aforementioned studies, include: security policies, physical security, network security, data security, and access control. According to the studies, when information security status based on all the key elements are established on the basis of implementation levels of all the elements as well as the sub-elements associated with each element, this could collectively be relied upon to portray the information technology security status for the entire information infrastructure in a given university, (Azuwa *et al.*, 2012).

Findings on the application of major elements of IT Security management

The study found that the major elements are used across the universities as a guide to managing IT security. It emerged that the major elements of IT security include: IT security policy, Physical security, Network security, data security and access control.

Information Technology Security Policy (SP)

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.

Table 1: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

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. 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 policy as a management document, which 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.

This is further confirmed by the results as summarized in the table, which shows that 60 percent of the respondents felt that the IT security policy in their universities do not effectively guide the behavior of the users of information systems. 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. 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.

From the relevant studies reviewed in the literature above, the information technology security policy informs all users of the requirements for system usage. Information security policy is stressed as the cornerstone for effective information security structure, (Peltier *et al*., 2005). The policy covers proper risk assessment mechanisms that help in exposing the vulnerabilities to information security and adoption of better security controls, (Hu, Hart, & Cooke 2012).

Further findings showed that among the systems users, the study shows that 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 the some of the universities sampled, violators of the policy do not face any consequence, hence such penalties remain unknown. 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.

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'.

The Element two: Physical security for information systems

This study found that only 32 percent of the universities implement signage effectively, while 68 percent do not, yet signage along key data lines and computing facilities is very important for ensuring information system security. 48 percent of the universities do effectively maintain IT systems asset register, while 52 percent do not maintain it effectively. 60 percent of the universities do not effectively control access to physical facilities hosting IT systems, while only 40 percent control the physical effectively. The study also found that 76 percent of the respondents agreed that the security of physical computing facilities are not effectively monitored through closed circuit television -CCTV, while only 26 percent of the universities, mainly the private universities do it effectively.

These results concur with Casey (2011), which showed that security levels in the environment surrounding computing facilities ought to be considered in universities. According to Carsey, facilities are kept in some forms of physical enclosures for security provision. These enclosures include behind the grills, perimeter fences and locked server - rooms, (Stallings & Brown 2008). Further, in support of these findings, Mitnick and Simon (2011) considered information systems, and concluded that physical security of computing tools is a crucial element of IT security. Moreover, he study's findings support Mang'ira and Andrew (2014), which highlighted that availability of information systems' resources in Universities in Kenya is affected not only by hacker activities, but also by physical security incidents like natural disasters, accidental and deliberate actions including: disconnection of network cables, computer theft, vandalism, floods, sabotage, fire, strikes/riots and lighting.

Element three: Network Security

Anderson (2001) showed that network security helps to safeguard confidentiality, integrity and full-time availability of the computing resources that it supports. 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) and Makori, (2013), that fast computer networks have made the universities' data to remain accessible and sharable faster and more widely than before and this exposes the entire university computing resources to the insecure world through the internet.

Table 2: 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**

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 the amount of internet subscribed in the evenings, throughout the nights and all aver 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.

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 problem by (Ismail and 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 Wi-Fi, 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 pass-word for all and any users within the universities to access the Wi-Fi.

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).

Table 3 : 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 multiple 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.

Element four: Data Security

Data security control practices in a university, for example: encryption, back-ups and restoration are necessary in an organization, (Bulgurcu, Cavusoglu & Benbasat 2010). This research showed that up to 60 percent of the universities successfully back-up their data, while 46 percent retrieve their data effectively after successful back-up. However, only 32 percent of the universities conduct full system back-up while 68 percent of the universities only do simple file back-up.

Data security continues to suffer from malware attack that compromises both data integrity as well as availability. For instance, Eira and Rodrigues (2009) showed that universities' networks are frequent sources of malware. The current study found that 64 percent of the universities do not effectively control malware in their systems. This is because up to 48 percent of the respondents admit unavailability of critical servers and applications due to malware attack. 49 percent of the users admit that there is no control on transferring data through portable external storage media like flash - disks and memory cards. This finding concur with Sandvik (2016), that malware spreads fast through such portable devices and this causes multiple losses to information resources, thus rendering information systems unavailable in institutions. The use of external portable storage media contributes so much to malware transfer from one computer system to another, and could be a major concern for data security within universities, Ismail and Zainab (2011). This study found that use of portable devices remains un-controlled within 48.9 percent of the universities in Kenya. The access to the university server room is much restricted in the universities, as 60 percent of the respondents indicated that it is very

difficult, as over 90 of the respondents showing that it is difficult. Only 47 percent of the universities operate on encrypted files and folders, while 53 percent do not.

The study further found out that academic and financial information were the most valued in the universities in Kenya at 33 percent and 37 percent respectively. Thus, 70 percent of universities attach great value to academic and financial information systems. This supports the Mahnic, Uratnik and Zabkar, (2002) study among the Slovenian universities that showed academic and financial information systems had much high levels of security as compared to other information systems within the university. Ndung'u 2015 and Casey (2011) noted that students and university personnel do compromise mainly academic and financial systems for their selfish interests. It was found that 62 percent of those sampled have lost data within the system, and which they successfully recover.

University has different types of data. Apart from data originated by the user through file generation, automation systems like student registration systems, ERP (enterprise resource planning), student finances and examinations systems are major sources of data, (Ndung'u 2015). According to Selwyn (2007), data classification is very important in determining the most critical data, and prioritizing security appliances' investment approach to apply. The findings in this research showed that 64 percent of the respondents confirmed that there is data classification in their universities, while 76 percent confirmed that they prevent data leak in their systems. The findings agree with Galliers and Leidner (2014) adding that data classification controls access, reduces data leak , guarantees data integrity and is applicable in most universities and other learning institutions.

Casey (2011) indicated that a server is of central necessity and has become the premier-most target such that access to it may mean compromising the security of the entire information system. Even though the facility is accorded physical security like metallic grills, perimeter fences and locked server - rooms, leaving the system attached to a ready to use accessories may mean easy and quick access into the entire information systems by unauthorized persons, (Stallings & Brown 2008). The study found that 56 percent of the respondents indicated that their critical servers were always attached to ready to use mice and key boards. This poses real risk of quick and easy unauthorized access into the server.

Data and system Back-ups

Data back-up helps in restoring operations in the event that primary computing data sources cannot be accessed. System back-up considers not only the data back-up, but also the entire application and repositories associated with the data. This is usually more reliable that data back-up since the secondary site acts as a hot site. The study found out that 76 percent of the respondents sampled from the universities conduct regular and automated data and systems back-up, as shown below. This is consistent with findings by Ismail and Zainab, (2011) study on Malaysian's special and public libraries that good backup policies and recovery procedures ensure information system's security.

Element five: System access control

Shelc, (2015) defines access control as the limitation of entry into an information system to only authorized persons, in order to safeguard confidentiality, integrity and availability of information asset. The Nyamongo (2012) noted that access control to information asset in universities in Kenya is affected by poor password usage and mismanagement of user-groups. Makori (2013) indicates that insiders have breached system access controls for information systems in the universities thus gaining un-permitted access.

This study found that 92 percent of the respondents showed that there is system's controlled password expiry within the universities as shown in below. It also found that bio-metrics and access control cards are rare authentication methods used in the universities to control access into the universities' server rooms. Only 12 percent showed that they use access control cards while 41.7 percent of the respondents indicated the use of bi-metrics to access university server rooms as only 16 percent incorporate the use of access passwords in the authentication.

Table 4 : Access control mechanism applied

	No	Yes
System controlled password	8	92
Bio-Metrics authentication	58.3	41.7
Access Control Cards authentication	88	12
Mixed / Combinations with passwords authentication	84	16

The study further found out that most universities still rely on physical access control mechanisms like the grills and physical locks to control access into the server rooms. Table 4.7 below shows that only 28 percent of the universities use system based authentication method. 72 percent of the respondents still use physical intervention approaches to control access into the server rooms.

Table 5: Nature of authentication used to access server room

Response	Percentage
System Based	28.0
Physical	72.0
Total	**100.0**

Conclusion And Recommendation

Conclusions

On security policy, up to 37 percent of universities in Kenya have not adopted IT security policy, yet the document is really substantial. The findings further indicated that up to 40 percent of the respondents do not feel any great impact of the information technology security policy in the universities, while 52 percent of the respondents showed that the policy does not effectively meet the industry requirement. Further over 64 percent of users are never trained regularly on IT security requirements as 72 percent of the respondents confirm that consequences of violating the policy are not effectively spelt out. This shows poor implementation of the major element of IT security - IT security policy in the universities.

On physical security, 32 percent of the universities implement signage effectively along critical data lines, only 48 percent of the universities do effectively maintain IT systems asset register, while

76 percent of the respondents agreed that the security of physical computing facilities are not effectively monitored even through closed circuit television -CCTV. The second major element of IT security is further poorly implemented within the universities.

On network security, more than 60 Percent of the universities are subscribing to above 100 Mbps internet bandwidth, which is an indication of high internet connectivity within the universities. 56 percent of the local

area networks in the universities are not hierarchical but flat, 72 percent have not effectively conducted penetration testing where security appliances exist, thus are not aware of the effectiveness of the security appliances employed. it was further found that 76 percent of the university networks do not have redundant core back-bones while 56 percent of the universities, apply one common and universal pass-word for all and any users within the universities to access the Wi-Fi.

On data security, 49 percent of the users admit that there is no control on transferring data through portable external storage media like flash - disks and memory cards. Only 47 percent of the universities operate on encrypted files and folders, while 53 percent do not. it was found that that 62 percent of those sampled have lost data within the system. On access control, 72 percent of the respondents still use physical intervention approaches to control access into the server rooms. there is limited application of computerized access control methods in the universities.

Recommendations

The study findings reveal inadequate concentration on IT security elements in managing IT security. It is recommended more focus be put on the above highlighted IT security elements to ensure better management of information security. The study recommends isolation of accessories like the mouse and keyboards from critical server, network segmentation, database authentication access control to wi-fi resources, file encryption and strict implementation of IT security policies.

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)*.

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

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

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.

Casey, E. (2011). *Digital evidence and computer crime: Forensic science, computers, and the internet*. Academic press.

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

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 Telecomunicaćões/Instituto Superior, Technical University of Lisbon.

Galliers, R. D., & Leidner, D. E. (Eds.). (2014). *Strategic information management: challenges and strategies in managing information systems*. Routledge.

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.

Luambano, I., & Nawe, J. (2004). Internet use by students of the University of Dar es Salaam. *Library Hi Tech News*, *21*(10), 13-17.

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

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

Mitnick, K. D., & Simon, W. L. (2011). *The art of deception: Controlling the human element of security*. John Wiley & Sons.

Mugenda, O. &Mugenda A.(2003). *Research methods: quantitative and qualitative approaches*.

Mukhwana, E. J., Kande, A., & Too, J. (2017). Transforming University Education in Africa: Lessons from Kenya. *African Journal of Rural Development*, *2*(3), 341-352.

Mullard, J. (207). Corrosion-induced cover cracking: new test data and predictive models. *ACI Structural Journal*, *108*(1), 71.

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

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.

Peterson, L. L., & Davie, B. S. (2007). *Computer networks: a systems approach*. Elsevier.

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.

Rubin, A., & Babbie, E. R. (2012). *Brooks/Cole Empowerment Series: Essential research methods for social work*. Cengage Learning.

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

Selwyn, N. (2007). The use of computer technology in university teaching and learning: a critical perspective. Journal of computer assisted learning,23(2), 83-94.

Shelc, R. (2015). Authorized Access and the Challenges of Health Information Systems.

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

Sridhar, S., & Govindarasu, M. (2014). Model-based attack detection and mitigation for automatic generation control. *IEEE Transactions on Smart Grid*, *5*(2), 580-591.

Tipton, H., & Krause, M. (2000). Information security management.

Veseli, I. (2011). *Measuring the Effectiveness of Information Security Awareness Program* (Master's thesis).