International Journal of Computer Applications Technology and Research
Volume 7–Issue 02, 63-77, 2018, ISSN:-2319–8656

Model for Information Security Governance Prediction in Public Universities in Kenya

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

Dr. Solomon Ogara
Department of Computer Science and Software Engineering
Jaramogi Oginga Odinga University of Science and Technology
Kisumu, Kenya

Dr. Samuel Liyala
Department of Information Systems
Jaramogi Oginga Odinga University of Science and Technology
Kisumu, Kenya

Abstract: Information is one of the most important assets in Organizations worldwide. To enable secure business operations, an organization must have an effective security governance strategy. The study focused on Information security governance in Public Universities in Kenya by establishing the current status of information security practices. Purposive sampling used to select seven (7) public Universities. A descriptive survey design, involving questionnaire was conducted to collect quantitative data. 394 respondents participated in the study. Data was analyzed using SPSS software. Correlation and multiple Regression analysis were obtained. The findings reveal that information security management's participation level is inadequate to deal effectively with information security governance threats, roles and responsibilities not well defined in support of information security governance practices. The research provides a comprehensive model for ensuring alignment of information security objectives with business objectives.

Keywords: Information Security; Information Security Governance; Risk Assessment; IT; Public Universities;

1. INTRODUCTION

Organizations today face universal revolution in governance that directly affects their information management practices. There is an increased need to focus on the overall value of information protected and delivered in terms of enabled services. Due to the high-profile organizational failures of the past years, legislatures, statutory authorities and regulators have created a range of new laws and regulations designed to force improvement in universities governance, security controls and transparency. Previous and new laws on information retention and privacy, coupled with significant threats to information and systems disruptions from hackers, worms, viruses and terrorists, have resulted in a need for a governance approach to information management, protecting the universities' most critical assets, its information and reputation [24]. Public universities in Kenya increasingly uses Information for essential business operations including, administration, teaching, learning and research activities. It is also evident that variety of devices such as desktop and laptop computers, Personal Digital Assistants (PDAs) and mobile/cellular phones, each with the capability to access information located at respective institution's data centers are typically being used. It is impossible to completely lock down these devices as the Universities are havens of free exchange of information that must uphold the principles of academic freedom. This freedom opens an attack space to information but the greatest challenge is to ensure that information and the systems are open and flexible, yet as secure as possible. One of the biggest challenges with university cyber security is the sheer amount of hacking that goes on in these environments. Schools have to deal with a unique mix of user levels, including students who are often young, and relatively trusting, and are not

employees of the organization so they are less controlled. Research shows that 90% of malware attacks originate through e-mail, various types of spoofing and spear-phishing campaigns that entice students and others to click on illegitimate links that can usher in a Trojan horse to do damage to a network system, or compromise the security of information. Many of these kinds of threats are costly, which leads to an inundation of hacker activity that schools have to keep on top of, by segmenting network systems, shutting down compromise parts of the system, or by some other high-tech means [32]. Until recently, most of the public universities have focused their security on protecting the Information technology (IT) systems that process and store the vast majority of information, rather than on the information itself. However, this kind of approach is too narrow to accomplish the level of integration, process assurance and overall protection that is required to ensure confidentiality, integrity and availability of information [24]. Information security governance is achieved by implementing suitable set of controls, including policies, processes, procedures, organizational structures, and software and hardware functions. These controls need to be established, implemented, monitored, reviewed and improved, where necessary, to ensure that the specific security and business objectives of the organization are met [20]. Information security main goal is to reduce adverse impacts on the organization to an acceptable level of risk. To ensure effective information security, Universities information management must establish and maintain a governance model to guide in the development and maintenance of a comprehensive information security programme. However, studies undertaken by [31] found that management do not understand the importance of information security, they do not give adequate support. There are risks of integrity and confidentiality violation which leads to universities having unreliable grading, financial loss and jeopardized reputation. A study done by [40] found that practices around information/data security elements were not to the expectation within the universities. Despite all these threats and risks, there is still a perception that information security is an IT problem rather than everyone's business. The purpose of this study is to design a model for Information security governance for public Universities in Kenya by establishing the current state of information security governance practices. The research model will enable the academia, business managers and information Technology practitioners rethink and review their ISG practices and ensure that Information security is placed at the executive management level in order to ensure that Information security and business objectives are aligned.

2.0 RELATED WORK

[17] defined the objective of information security as the protection of the interests of those relying on information, and the information systems and communications that deliver the information, from harm resulting from failures of availability, confidentiality and integrity. Any organization may consider the security objective met when those three criteria are satisfied, that is, when information systems are available to users at any given time (availability), data and information are disclosed only to authorize users (confidentiality), and data and information are protected against unauthorized modification (integrity). Given the dramatic rise of information crimes, including phishing and other cyber attacks, few today would contend that improved security is not a requirement. With new worms/malware and the increase in reported losses of confidential customer information and intellectual property theft, senior management is left with little choice but to address these issues. Information security requires a balance between sound management and applied technology. With the widespread use of networks, individuals and organizations are concerned with other risks pertaining to privacy of personal information and the organization's need to protect the confidentiality of information, whilst encouraging electronic business [22]. IT is essential for managing the information and knowledge required in the daily operations of an organization. It has, thus, become an integral part of most businesses and is vital to their growth [22]. Such growth comes at a price, however, today many security threats exist that threaten both IT and information per se [52]. Consequently, both IT and information have to be protected using proper information security measures that will ensure continued growth and derived benefit [21]. Casey [6] indicated that data security should be a key element of information technology security, that directly contributes to its measurement, data security controls like

encryption, back-ups and retrieval are therefore so important, that they are usually incorporated in the information security policy as well as metrics. [21] Illustrates that, information security is achieved by implementing a suitable set of controls that consist of policies, processes, procedures, organizational structures and software and hardware functions. The controls need to be established, implemented, monitored, reviewed and improved to ensure that the particular security and business objectives of the organization are met. This exercise should not be done in isolation but in conjunction with other business management processes. A comprehensive security programme implements the protection of information assets through a layered series of technological and nontechnological safeguards and controls like safety and environmental security measures, perimeter and physical security, background checks, access control security measures, user identifiers, passwords, IT technical measures and manual and automated procedures. These safeguards and controls are necessary and should address threats and vulnerabilities in a manner that reduces potential impacts to a defined acceptable level [21]. [27] on Corporate Governance helps to clarify why information security should be addressed as a corporate governance responsibility. Firstly, a major point of consideration is that the executive management is responsible and accountable to the shareholders of the company and therefore, they must ensure that their organization produces business value and delivers a suitable return on shareholder investment. Good information security efforts will most assuredly help to generate this return, which [45] clearly motivate. [27] Further states that executive management is responsible for ensuring that their organizations comply with all applicable laws, regulations and codes of best practice that should be well documented within a model. It should be in their best interest to fulfill this responsibility as failure in this regard could result in stringent legal action against them [45]. [4] Highlights two critical obstructions which hinder effective Information Security governance. Firstly, the responsibility for Information Security is frequently handed over to the Chief Information Officer (CIO), or the Chief Security Officer (CSO), who may not necessarily be positioned to delegate the resources and have the authority required to resolve various Information Security-related issues. Due to lack of attention by executive management, the allocation of finance to Information security efforts is scant in relation to the risks and degree of damage that security incidents may produce. Until the executive management has sufficient knowledge of the criticality of information security governance, inadequate support for security systems may be allocated less resources resulting in defective risk mitigation activities. More often than not, executive management only realizes the extent of information security risks after a severe incident occurs with severe consequences to the organizational reputation.

2.1 The Benefits of Information Security Governance

Information Security Governance (ISG) is a complex issue requiring the commitment of everyone in an organization to fulfill their role in protecting organizational information assets. Information security governance, if executed effectively, is of value to organizations in ways that exceed the mere observance of lawful conduct [45]. Effective information security governance results in enhanced internal security practices and controls and the promotion of self-governance as an alternative to legislation [11]. Sound ISG efforts have the potential to reduce auditing and insurance costs and differentiate the organization from industry competitors through an ongoing process of self-improvement [11]. ISG is a useful function for increasing overall productivity and lowering costs by delivering strategic alignment with broad organizational strategies and risk appetites [23]. This produces value for stakeholders, including by improving risk management efforts and enabling better performance measurements to provide assurance that information-related risks are under control [23]

2.2 Universities Information Security Threats

[28] States that universities face a variety of cyber security threats. These include disruption to the functioning of a university network, through to more general and targeted attempts to obtain valuable information from networks and their users. He further states that Universities also face a growing challenge from advanced, persistent and targeted threats that reflect the sector's important contribution to innovation and economic development worldwide. Cyber

security vulnerabilities are caused by a combination of the technical and human elements of a system. Technical elements may include software vulnerabilities that allow unauthorized access through a particular program. However, security failures are often traced to various forms of user vulnerability. Legitimate users may be targeted by social engineering that encourages them to take certain actions or divulge information that will allow attackers access to systems. Persistent remote access may also be achieved through unauthorized physical access to networks, such as through unsecured removable media like laptops or mobile devices. [28] Posits that the primary risk from the different types of cyber threat is to the business continuity of the institution, theft of information or damage to networks may have immediate impacts that prevent the university and its community from going about their work. Institutions or researchers may lose access to essential data or that data may become corrupted. However, information may also be stolen, including without the owner's knowledge, with eventual costs not realized until later. Recent highly publicized cyber attacks [15] have spurred a growing public awareness of the risk that sensitive personal information might be accessed by unauthorized third parties. Higher education since 2005, have been the victim of 539 breaches involving nearly 13 million known records. This trend 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. Federal Trade Commission promulgated its (FTC) Safeguards Rule. This rule, above all, directs institutions providing financial products or services to establish a comprehensive written information security program (WISP) containing administrative, technical and physical safeguards to protect customers' personal information. The FTC indicated that colleges and universities are subject to the Safeguards Rule [12]. [15] Further indicates that cyber attacks prove that even the most sophisticated computer systems like those of major banks, the government, and top retailers are not impenetrable. Higher education institutions are, unfortunately, no exception, in 2014 alone as many as 42 colleges and universities were victims of cyber attacks, and there have been at least eight in 2015. In 2009 at the University of California Berkeley, 160,000 people had their identity stolen during a computer security breach, the hackers operated for six months before being discovered [14]. [42] highlighted that about 53 universities, including Harvard, Stanford, Cornell, Princeton, Johns Hopkins, the University of Zurich and other universities around the world were hacked and about 36,000 e-mail addresses and thousands of names, usernames, passwords, addresses and phone numbers of students, faculty and staff from such universities were published to the Website Pastebin.com. Similar incidents have also been witnessed in public and private universities in Kenya. According to [50], Kenya is among African countries leading in cyber-attacks, just like Morocco, Egypt and South Africa. In October 2011, a report was circulated to all Vice Chancellors of public universities and Principals of University Colleges from the Office of the Permanent Secretary, Ministry of Higher Education, Science and Technology contained Information about a group of university students that compromised academic and financial systems' integrity by altering grades and fee balances in favor of students. The affected universities were reportedly among others; Jomo Kenyatta University of Agriculture and Technology, Daystar University, the Catholic University of Eastern Africa, and Maseno University. In yet another incident, on December 6th 2011, a syndicate of employees and students of Kenyatta University hacked into the institution's online database and altered examination results [46]. Due to the alterations, the university struck off names of many students who were scheduled to graduate on December 9th 2011. During the graduation period, students want better cumulated average score, and fee clearance as well, and this creates the motivation for attacking university systems [26] With this in mind, better security often starts with identifying separate pools of users for example, administrative staff versus faculty and students, and then customizing controls and access for each of these groups individually. The challenge of limited resources and funding for university cyber security generally speaks for itself. The above kinds of network monitoring and cyber security engineering have significant costs attached to them, and many universities simply find it difficult allocate the manpower or the funding to address cyber security issues. [53] Emphasized that failure of institutions to recognize the strategic importance and crucial role of electronic information assets as well as not ensuring its

protection can be seen as gross negligence in terms of good Corporate Governance. He went on further to argue that good Corporate Governance entails that all risks against electronic assets of the institution must be identified and properly managed. However, these actions belong to the Executive Management as part of their good Corporate Governance responsibilities.

2.3 Risk Assessment

Risk assessment is a key part of an effective information security management system. [35] States that to minimize information security threats, risk identification, analysis and mitigation is paramount. The Risk Assessment provides insight and guidance in developing an effective security strategy. Instead of assessing organizational risk a mile wide and an inch deep, the Risk Assessment focuses on assessing the implementation, effectiveness, and governance of information security controls. The outcome of this assessment is a prioritized analysis of risks and exposures that should be addressed to better protect your organization. This argument is also supported by [2] that once security risks have been identified and decisions for the treatment of risks have been made, appropriate controls should be selected and implemented to ensure risks are reduced to an acceptable level. Understanding risk helps organizations in any industry make more informed business decisions. This assessment helps executives determine what risk they are willing to accept, versus what risk should be mitigated through security improvements that will generate the most return on investment.

2.4 Information Security Controls

A security control is a safeguard or countermeasure designed to protect the confidentiality, integrity, and availability of an information asset or system and meet a set of defined security requirements. According to [48] Security controls cover management, operational, and technical actions that are designed to deter, delay, detect, deny, or mitigate malicious attacks and other threats to information systems. The protection of information involves the application of a comprehensive set of security controls that address cyber security (i.e., computer security), physical security, and personnel security. It also involves protecting infrastructure resources upon which information security systems rely (e.g., electrical power, telecommunications, and environmental controls). The selection and application of specific security controls are directed by a facility's information security plans and policies.

2.4.1 Physical Security Controls

Physical controls form the first level of defense for an organization. Such controls prevent access to facilities by unauthorized individuals [43]. Accordingly, these controls regulate access in and out of organizational environments. Such controls are the easiest and least expensive to implement, but are often also the most effective. Common physical controls include items such as walls, doors, fencing, gates, locks, badges, guards, bollards, cameras and alarm systems. [1] however, also mentions that physical controls include the measures required to maintain the physical environment in organizations, including heating, air-conditioning systems, fire-suppression systems, backup power generators, guards and receptionists, door access controls, restricted areas, closed-circuit television (CCTV), automatic door controls and human traps, physical intrusion detection systems, and physical protection systems. Many believe that physical controls do not play a vital role in an organization's security, but they are actually the most critical components [1] They can be considered critical owing to the fact that if one cannot guarantee or protect the physical environment in an organization, then any other controls that are added would be immaterial [1].

2.4.2 Technical/ Logical Security Controls

According to [3], technical security controls is also called logical controls, they refer to restriction of access to system. [44] Posits that logical security elements consist of those hardware and software features provided in a system that helps to ensure the integrity and security of data, programs and operating systems. Hardware elements that segregate core and thus present overlap, accidental or intentional, level of privileges that restrict access to the operating system programs, firmware programs that are not software- modifiable and similar Software elements that provide access management capabilities. These are the key security elements in a program to protect electronic information. An effective logical security system provides the means to identify, authenticate, authorize, or limit the authenticated user to certain previously stipulated actions, for each system user who may sign on or for each program

that may be called on by the computer to process files with established value factors. These include firewalls, access control lists, file permissions and anti-virus software.

2.4.3 Administrative Security Controls

Administrative security controls also called procedural controls are primarily procedures and policies which put into place to define and guide employee actions in dealing with the organizations' sensitive information [25]. They inform people on how the business is to be run and how day to day operations are to be conducted. Laws and regulations created by government bodies are also a type of administrative control because they inform the business. Administrative security controls in the form of a policy can be enforced with technical or physical security controls. For instance, security policy may state that computers without antivirus software cannot connect to the network, but a technical control, such as network access control software, will check for antivirus software when a computer tries to attach to the network. Administrative controls offer clear guidance; they include separation of duties, least privilege and user computer access registration and termination. Conducting security awareness and technical training to end users and system users helps in protecting the organizational mission. Administrative controls deal with implementation of personnel security controls including personnel clearance, background investigations, and rotation of duties, conducting periodic review on security controls and to employees on how they should act when confronted with a potential security breach [49]. Unfortunately, organizations have found that if they cannot enforce compliance with these controls, then their value is drastically diminished [1]. This often leads to a false sense of security where management of an organization trusts that its employees are operating in a safe and secure manner, but in actual fact they might not. This lack of compliance often results in serious consequences for organizations. It can therefore be stated that having controls that are not monitored or enforced is tantamount to having laws but no police [54].

2.5 Information Security Policy

According to [41], the cornerstone of effective information security architecture is a well written security policy. A security policy is a formal statement of the rules by which people who are given access to an organization's technology and information assets must abide. Since a policy is typically written at a broad level, organizations must also develop standards, guidelines, and procedures that provide employees with a clear approach to implementing the policy [37]. In order for a security policy to be appropriate and effective, it needs to have the acceptance and support of all levels of employees within the organization. The ISO 27001 standard requires that the security policy document (A.5) should be approved by management, published and communicated as appropriate to all employees [5]. It should state management commitment and set out the organizations approach to managing information security. However, [10] pointed out that good governance of Information Security is reflected by the commitment of the management and the leadership through formulation of a security policy based on risk analysis. Henceforth, security policy plays a strategic role in defining high level organizational direction, as well as being specific to the practical operations for users [30].

2.6 Information Security Governance Roles and Responsibilities

The importance of the structure and organization of the information security within an organization is essential for the success of an information security governance plan. Several codes of best practices for information security management stress the importance of having a proper information security organizational structure which includes the creation of an information security forum [51]. [33] Suggest that the information security governance forum should consist of representatives from mid-level to senior-level management from lines of business, IT, audit and risk. Information security is everyone's responsibility from the general members of staff all the way up through all levels of management to the board of directors [16] but if all employees involved do not understand their roles and responsibilities, the organization will not be able to protect the integrity, confidentiality and availability of its information. [47] argued that it is important that people understand the protection available to them when faced with threats [13] and also when they are the ones causing the threat to the organization. [56] Refer to employee violations which may be passive such as employees who are poorly trained, careless, unmotivated or who accidentally enter incorrect data values. Examples of such

behavior are the failure to change passwords regularly, failure to shred sensitive documents, delays in making data backups or failure to select strong passwords Employees may not understand that these actions may result in harm to the organization without them specifically intending to do so therefore, [55] agree with the International Federation of Accountants that clearly communicating individual roles, responsibility and authority is a major activity. All interested parties should be involved but ultimately the responsibility lies at the management level. They should have an understanding of why information security needs to be governed and that they also have several responsibilities to ensure that information security governance is in place [55].

2.7 Critical Success Factors for Information Security Governance

2.7.1 Management Commitment

Ultimate responsibility for managing information security is borne by corporate management, this provides the resources and sets the requirements on the basis of which the IT security manager promotes and coordinates security activities. The objects and activities of information security must be in line with the organization's business objectives and the requirement imposed by them. Senior management must take charge of this and provide visible support and show real commitment. To do this, they have to understand the seriousness of the threat that information risks pose to corporate assets. Further, they need to ensure that middle management and other staff fully grasp the importance of the issue. The organization's information security policy and objectives must be known by corporate employees as well as by external partners. Information security policy represents the position of senior management toward information security, and sets the tone for the entire organization. It is recommended that coordinating the organization's information security policy should be the responsibility of some member of top management. Encouragement should be given to the extensive application of information security within the organization and among its stakeholder groups to make certain that problems are dealt within an efficient and regular manner. When necessary, external professional assistance should be sought to keep abreast of advances, standards and values in the field. At the same time, this enables establishing forms of collaboration for potential security breaches. The key component of information security work is the visible support and engagement of senior management. In practical terms, this commitment involves allocating necessary funding to information security work and responding without delay tone situations. Nevertheless, swelling the Size of the information security organization is unwise, for a small organization is often more flexible and faster on the draw. A better alternative to enlarging security staff is to enhance information security skills and knowledge at all levels of the organization, because that is where the actual work processes are yet another way of showing management commitment. Is participation in arrange of information security-related events, which serves to underline the importance attached to the topic [21].

2.7.2 Compliance

Organizations have to demonstrate an information security policy that proves they have a range of steps and measures in place for compliance, if these policies are not adhered to, the regulators reserve the right to prosecute [21]). [21] and [19] emphasize the importance of complying with an organization’s policies, company standards and procedures, this is because human nature in general and employees in particular do not always conform to the wishes of executive management with regard to information security and secure information practices. [30] argued that university environment is made up of a mixture of corporate culture and academic freedoms, thus it is most likely that information security may be taken as disabling rather than enabling. Hence by carrying out security awareness programs, the culture of compliance should develop.

2.8 Conceptual framework for Information Security Governance

A conceptual framework for information security governance in public universities in Kenya was developed from best practice recommendations and guidelines in information security governance as suggested in various standards, guidelines and literature by information security researchers and practitioners. The proposed framework (Figure 1 below) served as a guide to the data collection process and was used to develop the data collection

instrument. The research adopted the following concepts in developing the framework: Computer security requires a comprehensive and integrated approach that considers issues both within and outside the computer security field [36]. Careful selection and implementation of managerial, technical and operational controls as well as an understanding of their interdependencies is an important information security management success factor . Control A.7.1.1 of the [21] standard guidelines and best practices recommendations for information management were used to develop the conceptual model.

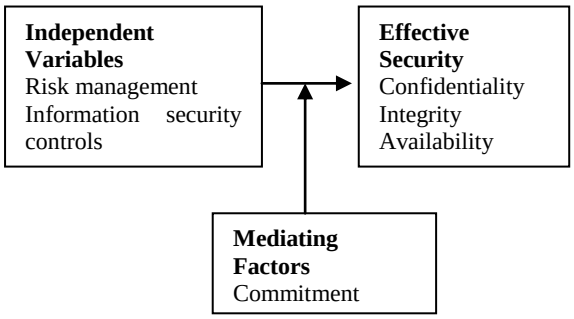

Figure 1. Conceptual Model

3.0 METHODOLOGY

The study adopted a descriptive survey design in which quantitative data was collected among employees of public universities in Kenya. 394 respondents were sampled using [57]. Purposive sampling was used to select the first seven (7) public universities that have been in existence for over ten years and have sound structure of governance that has evolved over time and where most of the other public Universities originated from as either constituent college or as a campus [8]. A Likert scale structured questionnaire was used to collect data from the executive management, security professionals and end users of the public universities. A Cronbach‘s Alpha value of 0.815 was obtained using SPSS. Content validity of the data collection instrument was determined by the subject matter experts who reviewed items adapted from relevant studies previously published in peer-reviewed journals. Correlation analysis was used to establish the relationship between the dependent and independent variables. Multiple Regression analysis was carried out to establish the strength of relationship between the predictors and the predicted. The outcome of the analysis was a model for prediction of Information security governance in Public Universities in Kenya. The confidentiality of the participants was ensured by not disclosing their names or personal information in the research, only relevant details that help in answering the research questions were included.

4.0 RESULTS

On risk assessment the findings shows that (60.4%) of respondents have documented risk management program to determine what controls can protect information, majority (78.8%) indicated that management has not identified and analyzed departmental risk relating to changes in operating environment, new personnel and new information systems, while (67.5%) indicated their key personnel fully consider risk in identifying potential dangers of information and systems, (42.1%) indicated that their institutions do not identify system weaknesses that could be exploited. As for security threats and vulnerability respondents indicated unauthorized access (82.7%) as a major threat to universities information security governance, others include social engineering (80.2%), IP spoofing (79.3%), Virus attack (71.8%), counterfeit software (68.9%), lack of file encryption (64.3%), lack of system backups (64.3%) and lack of awareness training (54.8%). As for information security policy the findings indicated that (62.7%) have their information security policies approved by top management, 74.4% indicated that the policies are communicated to them, violation of security policy not punishable at (81.7%). As for information security controls respondents indicated that physical security perimeter implemented (66.3%), no entry controls implemented (65.3%), user identification in place (75.2%), selection of strong password put in place (88.3%), no allocation of access rights (68.2%), no background investigation prior to employment(89.1%), installed Anti-virus (80.3%), termination of access right when job terminated implemented (74.9%). When respondents were asked on information security a governance responsibility , majority (74.6%) of the participants indicated that the IT Director and his team in the IT department are the ones responsible for maintaining the security program, 81.7% do not have information security roles stated in their terms and

conditions of employment, 60.4% no formally appointed a central point of contact for information security governance coordination and 71.9% no communication of business objectives for Information Security Governance Alignment to staff. A Pearson's correlation coefficient was then computed to establish the relationship between Public universities effective ISG and security best practices; a 2-tailed test significance value was used. A correlation coefficient for universities effective ISG with: information security controls was significant at r=.553, p<.01, Information policies significant at r=.394, P<.01, Risk management significant at r=.374, P<.01 and roles and responsibilities significant at r=.507, p<.01. Multiple regression analysis was computed to help predict trends, future values and to understand how much will the dependent variable change when independent variables changes. Multiple regression analyses was computed to understand whether availability can be predicted based on the predictors. A significant regression equation was found (P<.001) with R^2 = .400 as can be seen in table 1 model summary and Anova table 2 below. This means that 40 % of the variation in availability can be explained by the predictors.

Table 1: Model Summary for availability

Model	R	Rsquare	Adjusted Rsquare	Std.Error of the Estimate
1	.632[a]	.400	.384	.46018

a. Predictors: (Constant),Riskmgt_1,Sectrols_1, Rolesresponsi_1, Secpol_1

Table 2: Anovas for Availability

Model		Sumof Squares	df	Mean Square	F	Sig.
1	Regression	36.977	4	9.244	44.019	.000[b]
	Residual	56.521	268	.210		
	Total	93.498	272			

a. Dependent Variable: Availability
b.Predictors:(Constant),Riskmgt_1,Sectrols_1, Rolesresponsi_1, Secpol_1

A comparison across all statistics presented in Table 3 for the coefficients shows that; Information security controls (sectrols_1) has (B =.467, p <.001) ,Risk Management (Riskmgt_1) has (B =.210, p < .01), Information Security policies (Secpol_1) has (B =.189, p < .000), Roles and responsibilities (Rolesresponsi_1) has (B =-.143, p < .05) are all significant and their coefficients positive indicating that the greater the proportion of the predictors, the higher the availability of the effective model for information security governance.

Table 3: Coefficients for availability with Independent variables

Model		Unstandardized Coefficients		Standardized Coefficients	T	Sig.
		B	Std. Error	Beta		
1	(Constant)	-.058	.208		-.279	.780
	Riskmgt_1	.210	.076	.134	2.763	.006
	Secpol_1	.189	.065	.183	2.920	.004
	Sectrols_1	.467	.051	.475	9.113	.000
	Rolesresponsi_1	.143	.066	.133	2.161	.032

a. Dependent Variable: Availability

Multiple regression analyses was also computed to understand whether confidentiality can be predicted based on independent variable (Riskmgt_1, Sectrols_1, Rolesresponsi_1, and Secpol_1). From the results (R^2 = .583 as can be seen in model summary table 4, with a P= 0.000 as can be seen in ANOVA table 5). This means that 58% of the variation in Confidentiality can be explained by the independent variables.

Table 4: Model Summary for Confidentiality

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.764[a]	.583	.572	.54181

a. Predictors: (Constant), Riskmgt_1,Sectrols_1, Roles responsi_1, Secpol_1

Table 5: Anovas for confidentiality

Model		Sumof Squares	df	Mean Square	F	Sig.
1	Regression	108.886	4	27.221	93.865	.000[b]
	Residual	77.792	268	.290		
	Total	186.678	272			

a. Dependent: Confidentiality
b. Predictors: (Constant), Riskmgt_1, Sectrols_1, Rolesresponsi_1, Secpol_1

A comparison across all statistics presented in Table 6 of coefficients shows that; Information risk management has (B = .048, p < 0.001), Information security Policies has (B = .605, p < 0.001), Information security controls (Sectrols_1) has (B = .613, p < 0.001), Roles and responsibilities (Rolesresponsi_1), has (B = .357, p<.01) are significant and their coefficients positive indicating that the greater the proportion of predictors implemented the higher the confidentiality of the information security governance model.

Table 6: Coefficients for confidentiality with Independent Variables

Model		Unstandardized Coefficients		Standardized Coefficients	T	Sig.
		B	Std. Error	Beta		
1	(Constant)	2.441	.245		-2.895	.004
	Riskmgt_1	.048	.089	-.022	-.536	.002
	Secpol_1	.605	.076	.045	.856	.003
	Sectrols_1	.613	.060	.442	10.161	.000
	Rolesresponsi_1	.357	.045	.058	1.259	.008

a. Dependent Variable: Confidentiality

Multiple regression analyses was computed to understand whether integrity can be predicted based on independent variable (Riskmgt_1, Sectrols_1, Rolesresponsi_1, Secpol_1). From the results (R^2 = .422 as shown in table 7 model summary, P = 0.001 as can be seen in ANOVA table 8). This means that 42% of the variation in integrity can be explained by the independent variables.

Table 7: Model Summary for Integrity

Model	R	Rsquare	Adjusted Rsquare	Std.Error of the Estimate
1	.649[a]	.422	.407	.68894

a. Predictors: (Constant), Riskmgt_1, Sectrols_1, Rolesresponsi_1, Secpol_1

Table 8: Anovas for Integrity

Model		Sumof Squares	df	Mean Square	F	Sig.
1	Regression	91.773	4	22.943	48.918	.000[b]
	Residual	125.779	268	.469		
	Total	217.551	272			

a. Dependent Variable: Integrity
b.Predictors:(Constant),Riskmgt_1,Sectrols_1, Rolesresponsi_1, Secpol_1

A comparison across all statistics presented in coefficients table 9 shows that: Information risk management has (B = .498, p<0.001), Information security controls (Sectrols_1) has (B = .670, p<0.001), Roles and responsibilities (Rolesresponsi_1), has (B = .107, p< .05) are significant and their coefficients positive indicating that the greater the proportion of predictors implemented the higher the integrity of the information security governance model. Information security policies were not significant with information integrity.

Table 9: Coefficients for Integrity with Independent Variables

Model		Unstandardized Coefficients		Standardized Coefficients	T	Sig.
		B	Std. Error	Beta		
1	Constant)	-.136	.287		-.476	.635
	Riskmgt_1	.498	.061	.396	8.143	.000
	Secpol_1	.029	.089	.019	.324	.746
	Sectrols_1	.670	.071	.466	9.499	.000
	Rolesresponsi_1	.107	.053	.106	2.034	.043

a. Dependent Variable: Integrity

4.1 Information security governance model

To establish the relationship between public universities ISG model and information security best practices, a comparison across all statistics as presented in coefficients tables above shows that effective information security governance model has been defined in terms of Confidentiality, integrity and availability. The coefficients tables generally give the magnitude of the effects of the predictors variables have on the outcome which is the dependent variable. In the model the B value for each variable is considered, the coefficients for the model are in the B column and are determined using the Linear Probability model (LPM). The larger the B value, the greater the effect the predictor variable has on the ISG model. Using LPM, the model is arrived at by;

1. Confidentiality = 2.441 + 0.048(Riskmgt_1) + 0.605 (Secpol_1) + 0.613 (Sectrols_1) + 0.357(Rolesresponsi_1).
2. Integrity =0.136 + 0.498(Riskmgt_1) + 0.029 (Secpol_1) + 0.670 (Sectrols_1) + 0.357(Rolesresponsi_1)
3. Availability = -.058 + 0.210 (Riskmgt_1) + 0.189 (Secpol_1) + 0.447 Sectrols_1) + 0.143(Rolesresponsi_1)

To achieve effective information security governance, management must establish and maintain a model to guide the development and maintenance of a comprehensive information security programme. The relative priority and significance of availability, confidentiality and integrity vary according to the data within the business context in which they are used. For example, integrity is especially important relative to management information due to the impact that information has on critical strategy-related decisions and financial reporting. Confidentiality may be the most critical today as it relates to personal, financial or medical information, or the protection of trade secrets and

other forms of intellectual property (IP) and availability is when information is available and usable when required, and the systems that provide it can appropriately resist or recover from attacks.

5.0 DISCUSSION

The general objective of the research was to design an information security governance model for public Universities through the assessment of current state of information security governance in public university in Kenya. It is vital that public universities put appropriate controls, policies, risk management process, roles and responsibilities in place to secure information assets. A key to the protection of a company's information assets and the governance of the organizations is risk management. Enterprise risk management identifies information security risks that could impact the organization negatively. The outcome of this study revealed that 60.4% of the institutions have documented risk identification program is consistent with prior research on risk management which states that key to protection of organization's information asset and governance of information asset is having document risk identification program[16]. The ISO 27001 standard requires that the security policy document (A.5) should be approved by management, published and communicated as appropriate to all employees [5]. It should state management commitment and set out the organization's approach to managing information security. Most of the institutions 62.7% have their security policy approved by management, published and communicated at 74.4% as appropriate to all employees. Information security policy findings was consistent with prior research [37] which stated that information security policy should be documented by organizations as it is a plan identifying the organization's vital assets together with a detailed explanation of what is acceptable, unacceptable and reasonable behavior from the employee. In order to ensure security of information, the documented policies should not be violated [37. However, the findings show that 81.7% of the institutions violate policies and the violation of information security policy is not punishable. Based on this finding, it is important to help employees understand that non-compliance with Information security policies can cause serious information security problems for their organization. To address this issue, companies should organize information security seminars or training sessions to create awareness about information security threats and their severity. Institutions should also have a number of options for discreetly enforcing acceptable use of policies. For example, if IT discovers someone is viewing porn sites or chatting through Internet Messages all day, they can use firewall rule sets, router blacklists and content filters to block the prohibited activity. This keeps the violation quiet and preserves the person's employment. The findings therefore suggest that mitigation of risks can only be achieved through an information assurance programme that is built on solid strategic foundation defined by policy and not merely the implementation of malicious code prevention, firewalls or information security technologies. Information security policies are an important factor in determining the confidentiality of information assets. To exercise effective enterprise and information security governance, senior executives must have a clear understanding of what to expect from their enterprise's information security programme. They need to know how to direct the implementation of an information security programme, how to evaluate their own status with regard to an existing security programme and how to decide the strategy and objectives of an effective security programme [24]. From the finding of the study, 74.6% of the institutions security governance is left on the hands of security professionals. The finding is consistent with the [4] which showed that the responsibility for Information Security is frequently handed over to the Chief Information Officer (CIO), or the Chief Security Officer (CSO), who may not necessarily be positioned to delegate the resources and have the authority required to resolve various Information Security-related issues. This study shows that 81.7% of the institutions security roles are not stated in terms and conditions of employment an indication, which is consistent with [21] forum which stated that in most public organizations, information security governance responsibilities are loosely defined or not defined in most job descriptions, security performance is not a part of job reviews, most employees and even personnel themselves are not aware of good information security governance practices. Information security governance requires strategic direction and impetus. It requires commitment, resources and assignment of

responsibility for information security management, as well as a means for the top management to determine that its intent has been met. Experience has shown that the effectiveness of information security governance is dependent on the involvement of senior management in approving policy and appropriate monitoring and metrics coupled with reporting and trend analysis.

6. CONCLUSION

Information security governance is the responsibility of the senior executives. It must be an integral and transparent part of enterprise governance and be aligned with the IT governance framework. Senior executives have the responsibility to consider and respond to the concerns and sensitivities raised by information security, they are also expected to make information security an intrinsic part of governance, integrated with processes they already have in place to govern other critical organizational resources. The research reveals that information security governance desired outcomes cannot be achieved due to lack of senior executive management involvement. Accordingly, executive management is required to both direct and control information security according to sound corporate governance principles and list of information security best practices which include implementing various internal controls, policies, risk management strategies and mediating factors for information security to provide assurance that information asset are in a secure environment for business to thrive. The research reveals that most of these security best practices are rarely fulfilled due to lack of effective information security model for attention by executive management which will guide the executive management in the allocation of finance to Information security efforts in relation to the risks and degree of damage that security incidents may produce. To address this research gap, the study integrates a model for information security governance in public universities in Kenya with information security controls, policies, risk management strategies, defined roles and responsibilities. The findings strongly support the model, showing that all the security best practices ensured confidentiality, integrity and availability of information asset.

7. RECOMMENDATIONS

The study reviewed the current state of information security governance in Public universities in Kenya. The findings inform the research that information Security is still viewed as a technical aspect and not given any attention from the executive management. Due to lack of attention by the executive management Information Security has become reactive rather than proactive and poorly coordinated across the Institutions. The study recommends the executive management to rethink the way Information security should be addressed. They should be fully responsible for Information security in their institutions. They need to integrate information security into the corporate governance through the proposed model. The proposed model will help them have a reference point of acceptable of risks to information assets. Executive management should ensure the Information security is escalated to the boardrooms to be allocated enough resources just like other business assets. Proper information security governance is only possible on the basis of sound risk analysis, Public Universities should therefore use risk analysis as the basis for formulation of information security policy as well as selecting information security controls. Policy enforcement: Information security policy should be implemented and enforced to keep information secure. Password policies should be implemented and enforced to ensure the selection of strong passwords. The results of this study reveal that some users use weak passwords. Poor password selection is frequently a major problem for any system's security. Practically it can be challenging to ensure that staff and students have read, understood and complied with policies but the policies cannot be effective unless they are widely understood and enforced.

REFERENCES

[1] Andress, J. (2011). The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice. R. Rogers, Ed. Elsevier.

[2] Arnason, S.T., and Willet, K.D., (2008). How to Achieve 27001 Certification: An Example of Applied Compliance Management. New York: Auerbach Publications

[3] Bhaskar SM, Ahson SI (2008) Information Security: A practical Approach. Oxford: Alpha Science International Ltd.

[4] Business Software Alliance (2004). Information Security Governance towards a Model. available from: http://www.bsa.org/resources/loader.cfm?url=/commonspot.

[5] Calder, A. and Watkins, S. (2008). 4th Ed. IT governance: A manager's guide to data security and ISO 27001/ ISO 27002.

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

[7] Charles O. Oguk, C. Nickson Karie. N and Rabah, K. (2017). Information Security Practices in Universities in Kenya. Mara Research Journal of Computer Science & Information Security Vol. 2, No. 1, September 2017, Pages 61 - 73, ISSN 2518-8453.

[8] Commission of University Education (2013). Status of public Universities in Kenya and the ripple effects. Retrieved from http://www.cue.or.ke/status

[9] Cronbach, L. J. (1951). Coefficient alpha and the internal structure of tests. Psychometrika 16, 297-334.

[10] Elachgar, H. & Regragui, B. (2012). Information security, new approach. Innovative Computing Technology (INTECH), 2012 Second International Conference.

[11] Entrust, Inc., (2004). Implementing Information Security Governance (ISG). Available from: http://itresearch.forbes.com.

[12] Federal Trade Commission (2006). Identity Theft Survey Report, Synovate. Available at: http://www.synovate.com.

[13] Furnell, S., & Clarke, N. (2012). Power to the people? The evolving recognition of human aspects of security. Computers and Security, 2012, 983-988.

[14] Gilmore, J. (2009). Hackers attack campus databases, steal Social Security numbers, other data. http://www.berkeley.edu/news/media/releases/2009/05/08_breach.shtml.

[15] Harris, E. & Hammatgren, R. (2016). Higher education Vulnerability and cyber attacks: Establishing a written Information Security program to address exposure Available at: http://www.universitybusiness.com.

[16] Humphreys, EJ. Moses RH. and Plate EA. (2012). Guide to BS779 Risk Assessment and Management. British standard Institution (108).

[17] IFA, (2012). Pragmatic Security metrics. Applying metrics to information security International Security proceedings USA, 2012.

[18] International Federation of Accountants (1998). International Information Technology Guidelines—Managing Security of Information, USA, 1998.

[19] ISACA,(2012). COBIT 5 for Information Security. Available: https://www.isaca.org/COBIT/.*Documents/COBIT-5*-for-Information-Security-Introduction.pdf

[20] ISO/IEC 17799:2005: Information Technology – Security Techniques – Code of Practice for Information Security Management, ISO, Geneve (2005).

[21] ISO/IEC 27002 (2005). Information technology - security techniques - code of practice for information security management. Switzerland

[22] ITGI (2003). Information Security Governance: Guidance for Boards of Directors and Executive Management', USA, IT Governance Institute.

[23] ITGI (2005). Information Risks: Whose Business are they, IT Governance Institute.

[24] ITGI (2006). Information Security Governance: Guidance for Boards of Directors and Executive Management, Rolling Meadows, IL, IT Governance Institute.

[25] Jansson, K. (2011). A Model for Cultivating Resistance to Social Engineering Attacks.Nelson Mandela Metropolitan University.

[26] Karp (2016). *U.S. Patent No. D761,822*. Washington, DC: U.S. Patent and Trademark Office.

[27] King Report (2011). The king report on corporate governance, Available from http://www.iodsa.co.za

[28] Kritzinger (2013). Cyber security and Universities: Managing the risks, UK Government National Cyber Security strategy. www.universitiesuk.ac.ke

[29] Kritzinger, E. and Solms, S. (2013). A Framework for Cyber Security in Africa. JIACS, Vol. 3, pp.1-10.

[30] Lane, T. (2007). Information Security Management in Australian Universities - An Exploratory Analysis.

[31] Magomelo, M., Mamboko, P., Tsokota, T., (2014). The Status of Information Security Governance within State Universities in Zimbabwe. Journal of Emerging Trends in Computing and Information Sciences.

[32] Modern Malware Review (2017). Top 6 higher education security risks and Issues [online] available at: http://www.integrationpartners.com

[33] McMillan, R., & Scholtz, T. (2010). Security governance and operations are not the same.

[34] Ministry of Education (2007). Press Release By Hon. Minister For Education - Friday, 25th May 2007 on the eve of "2nd International Conference on ICT for Development, Education and Training - E-Learning Africa [online]. Available at: http://www.elearning-Kenyan_Ministry_of_Education.pdf.

[35] National Institute of Standards and Technology (1995). An Introduction to Computer Security: 88 The NIST Handbook, Special Publication 800-12 [online] Available at: http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf.

[36] National Institute of Standards and technology (1996). An introduction to Computer Security.

[37] National Institute of Standards and Technology (2003). Building an Information Technology Security Awareness and Training Program, Special Publication 800-50 [online] Available at: http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf.

[38] National Security Agency, USA. (2002).The 60 Minute Network Security Guide. First Steps Towards a Secure Network Environment.

[39] NIST - National Institute of Standards and Technology. 2013. Security and Privacy Controls for Federal Information Systems and Organizations.NIST Special Publication 800-53, Revision 4. Available at http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

[40] Oguk, C.O., Karie, N., Rabah, K. (2017). Information Security Practices in Universities in Kenya. Mara Res. J. Computer. Sci. Inf. Security. Vol. 2, No. 1, Pages 61 - 73, ISSN 2518-8453.

[41] Peltier, T.R., Peltier J., and Blackley J. (2005). Information security fundamentals.CRC Press.

[42] Perlroth, N. (2012). Hackers Breach 53 Universities and Dump Thousands of Personal Records Online. http://bits.blogs.nytimes.com/2012/10/03/hackers-breach-53-universities-dump-thousands-of-personal-records.

[43] Rainer & Cegielski (2010). Introduction to Information system: Enabling and transformation of Business. 3rd Edition Wiley and sons.

[44] Schweitzer J.A., (1990). Managing Information Security: Administrative, Electronics, and Legal measures to Protect Business Information. Boston: Butterworths.

[45] Swindle, O. and Conner, B. (2004). The link between information security and corporate Governance May 2004.

[46] The Star (2011). Student fails to stop KU graduation date [online] Available at: http://www.the-star.co.ke/national/national/52785-student-fails-to-stop-ku-graduation-date.

[47] Thompson K. and Von Solms R. (2006) Integrating Information Security in Corporate Culture, Port Elizabeth Technikon.

[48] United Nations Interregional Criminal Justice Research Institute. 2015b. Information Security Management System Planning for CBRN Facilities. United Nations Interregional Criminal Justice Research Institute, Turin, Italy.

[49] Vacca, J.(2009). Computer and Information Security Handbook. Elsevier

[50] Veseli, I. (2011). Measuring the Effectiveness of Information Security Awareness Program (Master's thesis). (Luambano & Nawe 2004).

[51] Von Solms, B. and Von Solms, R. (2004). The 10 deadly sins of Information Security. Management Computers & Security.

[52] Von Solms, R. and Von Solms, S.H. (2008). Information Security Governance. Springer International, USA: New York.

[53] Von Solms., B. (2006). What every Vice-Chancellor and Council Members should know about the use of ICT. CITTE Conference, 2006, Pretoria.

[54] West, R. (2008). The psychology of security. *Communications of the ACM*, *51*(4).

[55] Williams, P., & Andersen, A., (2001). Information Security Governance. Information Security Report, 6(3), 60-70.

[56] Willison, R., & Warkentin, M. (2013). Beyond deterrence: An expanded view of employee computer abuse. MIS Quarterly, 37(1), 1-20.

[57] Yamane, Taro (1995). Statistics: an introductory analysis. New York: Harper & Row