IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Vol. 8, Issue 5, May 2021

DOI: 10.17148/IARJSET.2021.8511

INFORMATION SYSTEM SECURITY CONTROLS AND DATA SECURITY IN UNIVERSITIES IN KENYA. A CASE OF KIRIRI WOMEN'S UNIVERSITY OF SCIENCE AND TECHNOLOGY

Ngethe Simon Ngugi[1], Tumuti Joshua[2]

Management Science, Kenyatta University, Kenya[1,2]

Abstract: Universities have adopted information systems replacing manual processes and thus simplifying work and increasing capacity which in turn has led to increased efficiencies. Information systems are useful in collection, processing, storage, retrieval and communication of information to the relevant users in a timely manner. Adoption of information systems come with the challenge of maintaining security. Various controls have been enforced to ensure that the systems are protected and thus enhance data confidentiality, integrity and availability. According to the United Kingdom General Data Protection Regulations, all data in a university must be protected from unauthorized access. However, data insecurity is still reported in many institutions of higher learning. Institutions are having challenges in monitoring revenue and tracking students' academic progress risking the credibility of the awards given while students are made to reseat examinations due to missing marks and pay fees already previously paid. This study sought to establish the influence of information systems security controls on data security in universities in Kenya. The study was guided by the following specific objectives; to determine the influence of administrative controls, technical controls and physical controls on data security in universities in Kenya. The study was carried out at Kiriri Women's University of Science and Technology. A descriptive research design was used for the study. Using purposive sampling technique, a sample of 55 respondents was included in the study drawn from the population of 122 information system users. The researcher used a questionnaire for data collection which was tested through a pilot study to establish the validity and reliability. The data collected was analyzed using the Statistical Packages of Social Sciences 21 (SPSS) program. Frequency distributions, percentages, correlation and regression analysis were computed and interpretations made. The findings were presented in tables and figures were be accompanied by detailed explanations. The studies established that administrative, technical and physical controls are correlated to data security in information system used in universities. From the data analysis, administrative, technical and physical control were all positively correlated to data security at; technical controls (r=.798, p=.000), physical controls (r=.575, *p*=.000) and administrative controls (r=.390, p=.005) at 0.05 significance level. Regression analysis established an adjusted R^2=.727 implied that 72.7% of the changes in the level of data security in the university's information systems can be explained by the changes in administrative, technical and physical controls. As such, enhancing these controls to a large extend help in mitigating data insecurity in information systems used in universities in Kenya.

Keywords: Data Security, Administrative Security Controls, Technical Security Controls, Physical Security Controls.

BACKGROUND OF THE STUDY

Information systems have increasingly replaced manual processes and thus simplified work, increased capacity and led to increased efficiencies in many organizations (Romero and Vernadat, 2016). Information systems are useful in collection, processing, storage, retrieval and communication of information to the relevant users in a timely manner. Information systems are comprised of hardware, software, databases, procedure, people and communication. In many modern organizations, most of the decisions made involve, at some level, the use of information systems (Pearlson *et al.*, 2016). According to Sumra et al., (2015), data security refers to maintaining data with high levels of confidentiality, integrity and availability. To ensure that such security is maintained, organizations place a wide range of measures referred to as information system security controls.

According to Tiffany *et al.*, (2019), universities have a challenge of data security and are attractive to unauthorized access due to their huge amounts of sensitive data such as financial information, academic information and intellectual property. Credibility of certification is a great concern due to missing marks cases whereby institutions lose track of students'

DOI: 10.17148/IARJSET.2021.8511

academic performance due to loss of data. Proper management of funds is also a major concern in all learning institutions in the world. Without effective information system security controls, money meant to support academic programmes and other budgeted uses is embezzled. According to Alsaleem *et al.,* (2018), information system security requires implementation of various information system security controls such as group securities, passwords, firewalls, encryption, mirroring and load balancing among others. This high level sophistication requires highly specialized personnel and high initial expenditure. Despite the huge capital outlay, major international learning institutions still report some level of data insecurity. In many developing nations, information systems have been adopted in an effort to match the trends and to realize the benefits of such systems. Nevertheless, due to of lack of sufficient technical knowhow and financing, there are inadequate information systems security controls (Abomhara, 2015). As a result, cases of unauthorized access to higher learning information systems have been rampant which has led to loss and exposure of sensitive information.

I) Information Systems Security Controls:

Information systems security controls are the measures that are undertaken to ensure that information system are secured from unauthorized access and are protected from attacks that threaten their existence and use (Arhin and Wiredu, 2018). Information system security controls seek to prevent and mitigate risks as well as handling the effects of information systems risks associated with accidental or deliberate unauthorized access to information system. Such I.S security controls protect the various components of an information system including the data held in the databases, individual user computers and secondary storage devices. By considering the nature of the information system controls, I.S controls are classified in the following ways; administrative controls, technical controls and physical controls (Yau, 2014). Information systems security controls are adopted to safeguard the data held in the information systems as well as the hardware and the softwares.

Administrative security controls consist of the policies (guidelines) and procedures set by the management to be followed by information systems users to deal data security risks (Choi, 2016). According to Yaokumah (2017), administrative security controls are extremely important since they determine the success of technical and physical security controls. For instance, the password policy is an administrative security control that enables information system users to understand how to effectively manage and use passwords which is a technical control for enhanced data security. As such, administrative security controls provide the regulations governing how information systems and other data security controls ought to be utilized in an institution. According to Yau (2014), data management policy, password management policy and division of duties policy are among the most popular administrative security controls used in higher learning institutions. Wara and Singh (2015), posit that even though administrative controls such as ICT policies are established, there is still data insecurity reported in much institution.

Technical controls are of paramount significance because they help in protecting data even if information systems are physically accessible by authorized users. According to Chang and Ramachandran (2015), technical security controls are either incorporated in the system during the system development stages by system developers or after implementation by the system users. According to Soomro and Ahmed (2016), technical security controls involve the use of hardware and software to enhance data security. These controls ensure that data is not accessible by unauthorized people or mishandled. These controls are effective because they are less subjectively interpreted unlike the administrative controls. Such controls help in identification, authentication and authorization thus ensuring that the data security is not deliberately or accidentally compromised. Technical security controls require higher technical knowhow to implement develop but can be used even by information systems users without high technical competence. Popular technical security controls used in many higher learning institutions include; logical access control through passwords and biometric scanning, encrypting, antimalware softwares, cloud computing and firewalls (Dave and David (2019).

Physical security controls prevent unauthorized physical access to the information systems' environment (Khajouei *et al.,* (2017). These controls help to ensure that there is no physical harm or abuse of information systems facilities including the information data storage devices. According to Huang and Serpanos (2018), physical security controls may include secure server rooms, lock and key, surveillance, installation of burglary and fire alarms. Such controls may prevent theft which may make the data unavailable when needed thus compromising data security. In that case therefore, physical security controls offer the first line of defence from unauthorized access to data held in information system. Physical security controls are implemented to complement other forms of security controls to better secure information systems (Carney, 2011).

II) Information System Security Controls and Data Security:

Information systems security controls are implemented because of the vulnerabilities of the systems and the risks of access that information systems always face. According to Ashibani and Mahmoud (2017), I.S security controls limit access to the physical facilities, access to databases and modification of data by unauthorized people. The information system data security risks cannot be fully eliminated but having the right controls significantly help in ensuring that confidentiality, integrity and availability of data in maintained. This is achieved by establishing a wide range of I.S security controls to deal with varied information system security risks. Therefore, I.S security controls are used to prevent, mitigate and to handle the effects of threats that have already occurred are required (Safa & Von, 2016).

According to Ashibani and Mahmoud (2017), institutions need to implement a wide range of effective controls in order to enjoy data security. According to Omito (2016), institutions of higher learning have had to set up proper information systems security controls in order to support the e-learning models which help institutions to remain competitive. As such institutions enact policies which govern; division of duties, password management, secondary storage media management, data management, procedure of entering and updating students' academic and financial information. Institutions also implement technical controls such cloud computing, anti-malware softwares as well as access control using password and firewalls. Physical security controls are implemented to restrict physical access to the information systems. Physical security controls include setting up secure server rooms, backing up, locking computer hardware in secure places and surveillance (Yau, 2014).

Many higher learning institutions; universities and Technical and Vocational Education Training (TVET) institutions have experienced numerous challenges in establishing effective information systems. Some institutions' information systems have simple databases which can easily be accessed by anyone with basic computer application literacy. More specialized academic programmes in these higher learning institutions have helped information technology students and specialists' device and implement better information systems security controls. However, as the knowledge increases, more sophisticated crimes have also been devised and therefore the data security challenge remains (Jalang'o, 2015).

According to Lehto (2018), appropriate information systems security controls in institutions of higher learning ensure that confidential and sensitive information is protected from authorized people. For instance data on academic progress is made unavailable to those who do not require it in their normal work routines. This mitigates the probability of the data being abused. I.S security controls also help is preventing modification of data by unauthorized people and maintain log that acts as an audit trail showing which information system user who edited the data and when the previous data that was edited (Wara and Singh, 2015). Securing information systems with effective controls also enables users to always access the data at minimal latency. To enable data access on demand, measures such as load balancing, mirroring and firewalls are utilized.

B. Statement of the problem

Adoptions of information systems in organizations including higher learning institutions come with the challenge of maintaining security (Sharma *et al.,* 2016). For institutions of higher learning to be considered to have secured data, the data should be unavailable to unauthorized users, data must be protected from unauthorized modification and data should be available on demand by the information system users (Sumra et al,. 2015). Various controls have been undertaken to ensure that the information systems are protected and thus enhance data security. These efforts notwithstanding, data insecurity is still reported. Wagdy (2017) states that African counties such as Kenya, Uganda, Botswana and Ghana are facing increased data insecurity in their higher learning institutions and advocates for more effective security controls. According to Jalang'o (2015), many Kenyan higher learning institutions are not able to fully track students' academic performance and missing marks are often reported. This is a problem of data unavailability in data security sense. Such insecurities have also led to huge financial losses to the affected institutions or placed a burden to learners to pay fee already paid but cannot be accounted for.

This is a grave situation since insecurity of sensitive information systems lead to huge losses, law suits and reduced credibility of academic awards from higher learning institutions Jalang'o, 2015). Regardless of the magnitude of this topic, very few studies have been done on this area. The few that have been done have not comprehensively looked at how the administrative, technical and physical controls impact on data security in higher learning institutions. In view of this, this study will seek to establish the influence of information system security controls on data security in institutions of higher learning in Kenya.

C. Objectives of the Study

I) General Objectiv:

Evaluating information system security controls and data security in universities in Kenya.

II) Specific Objectives:

i. To determine the influence of administrative controls on data security in universities in Kenya.
ii. To evaluate the influence of technical controls on data security in universities in Kenya
iii. To determine the influence of physical controls on data security in universities in Kenya.

RESEARCH METHODOLOGY

D. Research Design

This study adopted a descriptive research design. This design was used because according to Kim and Bradway (2017), it enables the researcher to collect data describing the characteristics as they are. The researcher was in a position to collect data on the prevailing situation and describe the information systems security controls and the state of data security

DOI: 10.17148/IARJSET.2021.8511

in institutions of higher learning as it is. Descriptive research design was non-experimental and therefore did not involve manipulation of the variables by the researcher.

The design enabled the researcher to identify the existing information system security controls in universities and the nature and frequency of data insecurity cases. This design enabled the researcher to use descriptive and inferential statistical methods to make generalizations. This was ideal since the research was concerned with conditions that already exist and practices that are held. In addition, the design enabled the researcher to collect data within a short time from all the respondents to be included in the sample.

E. Target Population

Population can be defined as all people or items that one wishes to understand (Rahi, 2017). The target population of this study was information systems users in Kiriri Women's University of Science and Technology. These included all the teaching staff and the administrative staff in the university. This was a total of 122 information system users.

F. Sampling Procedure and Sample Size

I) Sampling Procedure:

Sampling is the process of selecting the segment of the population to be investigated (Rahi, 2017). Sampling was done as it would be extremely difficult to reach the entire population and give findings in good time to influence policies for better data security in universities in Kenya The researcher endeavoured to ensure that the sample included respondents knowledgeable about existing data security controls. The researchers used stratified sampling technique in which the population was divided into two stratas, teaching and administrative staff. Using the Slovin's formulae $n = \frac{N}{1 + Ne^2}$ where n = no. of individuals in the samples, N = total population and e = margin of error (0.1), the number of information users to be included in the study was calculated.

Simple random sampling was used sampling technique was adopted to identify the individuals that were included in the sample.

II) Sample Size:

According to David (2017), a sample is the group of elements that actually participate in a study. Using the Slovin's Formulae, from a population of 122 information systems users, a sample of 55 respondents was included in the study.

TABLE 1 SAMPLE SIZE

	Number of Staff	**Percentage of staff**
Teaching staff	39	71%
Administrative staff	16	29%
Total	55	100%

Source: Author (2021)

G. Data Collection Instrument

The study utilized the questionnaire to collect primary data. Nassaji, (2017) identified the questionnaire as an ideal instrument for data collection for a descriptive research. The questionnaire was the ideal data collection instrument considering the busy work schedules of the staff in universities. The questionnaire was structured with both open ended and closed ended questions that enabled the research collect detailed quantitative and qualitative data. The questionnaire comprised of questions which helped to gather data related to the objectives of the study. The questionnaire was divided into sections in which each specific objective was effectively interrogated through a series of relevant questions.

H. Data Analysis and Presentation

According to Pitarch, Sala, & Prada (2019), data analysis is the process of systematic of inspecting, cleaning, transforming, and modeling data with the goal of discovering useful information, suggesting conclusions, and supporting decision-making. The data was analyzed using both qualitative and quantitative approaches in order to maximize the strengths of the research findings. The data was analyzed using the Statistical Package for Social Sciences (SPSS). The data was keyed into the computer, cleaned and analyzed to present the findings required for the study. Frequency distributions, percentages, measures of central tendency and dispersion and correlation and regression analysis were computed and interpretations made. The findings are presented in tables and figures. The figures offered graphical and visual representation of data that enabled to put across important information at a glance. Tables and figures were accompanied by detailed explanations of the research findings. A conclusion was drawn and recommendations made for future research on the same area.

DOI: 10.17148/IARJSET.2021.8511

DATA ANALYSIS AND INTERPRETATIONS

A. Introduction

This chapter presents the findings of the research. At the outset, the chapter gives the background to the respondents by analysing their demographic information. The results are presented in tables and figures and interpretations made in the context of the study. The chapter also presents the reliability, descriptive statistics, normality tests, relationship between the information system security controls and data security and the influence of information system security controls on data security.

B. Response Rate

The study targeted 55 potential participants across Kiriri Women's University of Science of Technology (KWUST). However, 51 participants dully filled and returned the questionnaires to the researcher for data analysis representing a response rate of 93%.

C. Descriptive Statistics

I) Means and Standard deviations:

The research sought to find out the means and standard deviations for every study variable. In order to achieve this, the composite values computed for each variable were used. The findings were as presented in Table II below.

TABLE II MEANS AND STANDARD DEVIATIONS

	Mean	Std. Deviation
Admn_controls	4.3950	.29910
Physical_controls	4.2770	.26018
Tech_controls	3.7451	.40310
Data_security	4.1793	.40455

n=51
Source: Author (2021)

The data collection instrument employed a likert scale in which respondents indicated the extent to which they agreed or disagreed with the statements that were used to measure the study variables. The responses were; Strongly Disagree (1) Disagree (2) Don't know (3) Agree (4) and Strongly Agree (5). The findings in Table 4.6 also showed that the means of the responses that were computed thereof for administrative, physical, technical security control and data security measures were; 4.3950, 4.2770, 3.7451 and 4.1793 respectively. The average means of above 4.00 suggested that respondents had confidence that the measures used would help in enforcing data security in the University.

The results in Table II also showed the standard deviations in the responses given for the scales used for each study variable. The standard deviations for administrative, physical, technical security control and data security measures were; .29910, .26018, .40310and .40455. The findings showed low standard deviations for all data sets which indicated that the values were close to the means of the sets. Therefore, most of the respondents showed agreement with the statements that measured administrative, physical, technical security control and data security.

D. Normality Tests

Normality is described by a symmetrical bell shaped curve that has the greatest frequency of scores in the middle and lesser frequencies towards the edges (Biswas & Bisaria, 2020). Normality tests were used to find out whether the sample was drawn from a normal distribution before performing other analysis. Normality tests was conducted for the data on the dependent variable, data security. The researcher used a normal Quantile-Quantile (Q-Q) plot.

I) Test of Normality Using the Quantile-Quantile Plot:

In order to affirm that the data was drawn from a sample obtained from a normal population, Quantile-Quantile Plot was generated. A Q-Q plot helps to identify whether there are outliers in the sample included in the study. The Q-Q plot generated was presented in Figure 4.4 illustrated below.

DOI: 10.17148/IARJSET.2021.8511

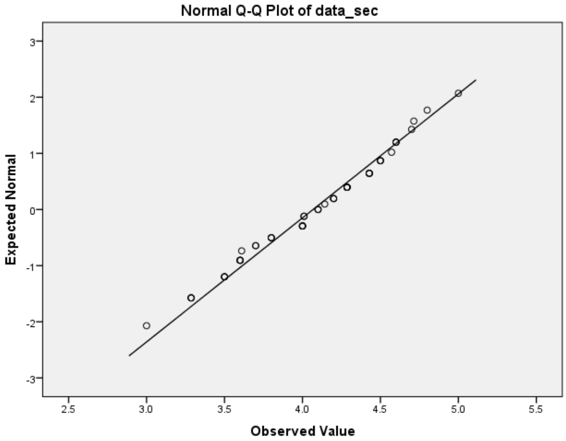

Figure 1 Test of Normality Using the Quantile-Quantile Plot
Source: Author (2021)

The pictorial representation of the distribution of data shown in Figure 1 shows the expected normal plotted against the observed normal. Figure 1 suggests that the data is normally distributed since non on the plotted points are far away from the line of reference.

E. Relationship Between Information System Security Controls and Data Security

The researcher sought to establish the relationship between information system security controls and data security in universities in Kenya. In order to establish the relationship between independent variables and the dependent variable, the researcher carried out correlation analysis.

The correlation was between the independent variables; administrative, technical and physical security controls and the dependent variable; data security in information systems.

TABLE III CORRELATIONS BETWEEN INFORMATION SYSTEM SECURITY CONTROLS AND DATA SECURITY

		data_sec	tech_controls	physical_controls	admn_controls
data_sec	Pearson Correlation	1	.798**	.575**	.390**
	Sig. (2-tailed)		.000	.000	.005
	N	51	51	51	51
tech_controls	Pearson Correlation	.798**	1	.395	.218
	Sig. (2-tailed)	.000		.004	.124
	N	51	51	51	51
physical_controls	Pearson Correlation	.575**	.395	1	.278
	Sig. (2-tailed)	.000	.004		.048
	N	51	51	51	51
admn_controls	Pearson Correlation	.390**	.218	.278	1
	Sig. (2-tailed)	.005	.124	.048	
	N	51	51	51	51

**. Correlation is significant at the 0.01 level (2-tailed).

*. Correlation is significant at the 0.05 level (2-tailed).

Source: Author (2021)

Results in Table III suggest that all the information systems security controls implemented had a positive correlation with data security in the institution. The correlation between information security controls and data security were as follows; technical controls (r=.798, p=.000), physical controls (r=.575, *p*=.000) and administrative controls (r=.390, p=.005). At 0.05 significance level, technical controls, physical controls and administrative controls were significantly correlated to data security in information systems in universities in universities in Kenya since they had a *p*<.05. However, despite the positive correlation between administrative controls and data security, the correlation was weak since r=.390.

The results in Table III suggest that as technical, physical and administrative security controls were enhanced, data security improved in the institution. Nonetheless, the implementation administrative security controls, have least impact

DOI: 10.17148/IARJSET.2021.8511

on the level of data security in the University. The findings of this study that are in-line with the findings of McIlwraith (2016) who posited that technical controls are most critical in ensuring data security in any information system. Menard *et al.,* (2017) had established that technical controls are of utmost significance in data security identifying passwords as the frontline defence in safeguarding data in an information system.

F. The influence of Security Controls on Data Security

I) Significance of the Model:

The study objectives were to determine if there was a significant relationship between the three predictor variables of Administrative Controls, Technical Controls and Physical Controls and the dependant variable of Data Security. Consequently, multiple regression analysis was performed with the aid of SPSS V20. Pitarch *et al.*, (2019) identifies multiple regression as ideal in establishing the extent to which independent variables explain the changes in the dependent variable.

TABLE IV ANALYSIS OF VARIANCE

Model		Sum of Squares	Df	Mean Square	F	Sig.
1	Regression	9.461	3	3.154	45.371	.000[b]
	Residual	3.267	47	.070		
	Total	12.728	50			

a. Dependent Variable: data_sec

b. Predictors: (Constant), physical_controls, administrative_controls, technical_controls

Source: Author (2021)

The findings in Table IV suggest that the overall regression model was significant, F(3,47)=45.4,p<.001, R^2=.743 as presented in Table V below. Therefore, the regression equation predicts the dependant variable. That is; administrative, technical and physical controls are significant predictors of data security. This implies that changes in the level of data security in the university's information system can be explained by the changes in the levels of administrative, technical and physical controls.

II) The Strength of the Relationship Between Information System Security Controls and Data Security:

In order to establish how the effect of information system controls on data security in universities in Kenya, the researcher conducted a multiple regression analysis. Table V shows the model summary.

TABLE V MODEL SUMMARY

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.862[a]	.743	.727	.26365

a. Predictors: (Constant), physical_controls, administrative_controls, technical_controls

Source: Author (2021)

Table V shows that administrative, technical and physical security controls are significant predictors of data security. Table V further shows an adjusted R^2=.727, taken as set predictors of Administrative security controls, technical security controls and physical security controls account for 72.7% of the variance in data security. This implies that 72.7% of the changes in the level of data security in the institution can be explained by the changes in administrative, technical and physical security controls. In view of this, the information systems security controls adopted were effective in enhancing data security in the institution.

III) Regression Coefficients:

The study used the coefficients table to establish the contribution of each predictor in the model. The findings were presented Table VI.

DOI: 10.17148/IARJSET.2021.8511

TABLE VI COEFFICIENTS

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	Collinearity Statistics	
		B	Std. Error	Beta			Tolerance	VIF
1	(Constant)	-1.372	.431		-1.875	.037		
	admn_controls	.291	.131	.172	2.223	.031	.909	1.100
	tech_controls	.547	.068	.654	8.073	.000	.831	1.203
	physical_controls	.520	.160	.268	3.255	.002	.805	1.242

a. Dependent Variable: data_security

Source: Author (2021)

The findings in Table VI suggest that all the three predictors (administrative controls, technical controls and physical controls) offer significant amount of unique variance in explaining the dependant variable. All the three predictors had a p=<.05; administrative controls sig. (p=0.31), technical controls sig. (p<.001) and physical controls sig. (p=0.02). Muliple linear regression thus was computed as shown in the expression below;

Data security= (-1.372)+.547(TC)+.520(PC)+.291(AC) where TC=Technical controls, PC =Physical controls and AC=Administrative controls. This implies that Technical Controls have the greatest impact on data security, followed by Physical Controls. Administrative Controls have the least impact on data security. The result of the study disagree with the findings of Yaokumah (2017) who found out that administrative controls have the greatest impact on data security since they determine the success of technical and physical controls. However, the findings agree with Soomro *et al.*, (2016) who established that technical controls most significantly impact on data security since they are less subjectively interpreted and can be enforced uniformly by all information system users.

SUMMARY, CONCLUSION AND RECOMMENDATIONS

A. Summary

Information system security controls play an important role in safeguarding the data maintained by the Kiriri Women's University of Science and Technology. The University employed a wide range of security control measures in order to enhance data security. The study established that the technical and physical controls implemented by universities to a great extent helped in enforcing data security in the Institution. The university had implemented software based measures that helped mitigate data vulnerability in information systems. The university used strong passwords that could not be easily guessed, implemented firewalls, used data encrypting and antimalware. Physical security controls implemented also significantly enhanced data security in the institution. These measures included; the use of separate server room, use of powerful servers, locking of work stations, locking of storage devices and surveillance of work station through the use of CCTV systems.

B. Conclusion

Information systems security controls are critical in ensuring that data is protected from unauthorised access, unauthorised modification and unavailability to the right users in Kiriri Women's University of Science and Technology. Having a sound ICT policy that outline how data should be managed was of paramount significance. Technical controls helped in protecting the data from threats that could not be easily detected by users in the University such as unauthorised remote access. Physical controls also helped in safeguarding data through basic measures such as locking the doors to work stations or rooms with computers and data storage devices in the University. Administrative, technical and physical security controls ensured that the students always had updated academic and accounts record, lecturer maintained accurate records, the institution did not lose revenue and litigations due to mishandling of data are avoided by the Institution. As such, the information systems security controls supported the University in achieving its objectives in an effective and efficient manner by ensuring data security.

C. Recommendations

Universities should enhance data security by including more measures to protect the information systems from different types of threats. Most importantly, the ICT policies used should clearly guide on how the data held in the information systems is to be protected. Beyond having rules and procedures, the management should rally support from the information system users in safeguarding the data. Technical controls such as the use of passwords, anti-malware, firewalls and data encrypting are critical measures of protecting data and therefore, universities should capitalise on them to enhance data security. Other scholars in future should conduct further studies to establish other factors not covered by the current study have an impact on data security in university information systems such as electrical problems.

DOI: 10.17148/IARJSET.2021.8511

REFERENCES

Abomhara, M. (2015) Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks. Journal of Cyber Security and Mobility, 4(1), 65-88.

Alsaleem, L. S., Aldakheel, M. F., Alotaibi, D. A., Alqahtani, S. A., Alharbi, S. F., & Nagy, N. (2018, April). Policy, Legal, Legislation and Compliance Saudi Personnel Compliance and Adaption to Recent Security Measures. In 2018 21st Saudi Computer Society National Computer Conference (NCC) (pp. 1-5). IEEE.

Arhin, K., & Wiredu, G. O. (2018). An organizational communication approach to information security. The African Journal of Information Systems, 10(4), 1.

Ashibani, Y., & Mahmoud, Q. H. (2017). Cyber physical systems security: Analysis, challenges and solutions. Computers & Security, 68, 81-97.

Carney J., (2011) Why Intergrate Physical and Logical Security Controls. Cisco Government and Security Solutions. Cisco systems. San Jose

Chang, V., & Ramachandran, M. (2015). Towards achieving data security with the cloud computing adoption framework. IEEE Transactions on Services Computing, 9(1), 138-151.

Choi, M. (2016). Leadership of information security manager on the effectiveness of information systems security for secure sustainable computing. Sustainability, 8(7), 638.

Dave Bourgeois and David T. Bourgeoi 2019 Information Systems for Business and Beyond. Information Systems Security journal. [online]

https://bus206.pressbooks.com/chapter/chapter-6-information-systems-security/Huang, W., Tang, W., & Beedgen, C. F. (2015). U.S. Patent No. 9,031,916. Washington, DC: U.S. Patent and Trademark Office.

Jalang'o, I., (22 August 2015) Missing marks hauting Kenyan universities: htttps://www.google.com/amp/s/www.standardmedia.com

Khajouei, H., Kazemi, M., & Moosavirad, S. H. (2017). Ranking information security controls by using fuzzy analytic hierarchy process. Information Systems and e-Business Management, 15(1), 1-19.

Kim, H., Sefcik, J. S., & Bradway, C. (2017). Characteristics of qualitative descriptive studies: A systematic review. Research in nursing & health, 40(1), 23-42.

Lehto, M. (2018). Cyber Security Education and Research in the Finland's Universities and Universities of Applied Sciences. In Cyber Security and Threats: Concepts,
Methodologies, Tools, and Applications (pp. 248-267). IGI Global.

McIlwraith, A. (2016). Information security and employee behaviour: how to reduce risk through employee education, training and awareness. Routledge.

Menard, P., Bott, G. J., & Crossler, R. E. (2017). User motivations in protecting information security: Protection motivation theory versus self-determination theory. Journal of Management Information Systems, 34(4), 1203-1230.

Mohamad, J., Ismail, S., Iman, A. H. M., & Mohd, T. (2019). Testing the Use of Multiple
Regression Analysis and Rank Transformation Regression for Heritage Property Valuation. Asian Journal of Quality of Life, 4(15), 42-62.

Nassaji, H. (2015). Qualitative and descriptive research: Data type versus data analysis.

Pearlson, K. E., Saunders, C. S., & Galletta, D. F. (2016). Managing and Using Information Systems, Binder Ready Version: A Strategic Approach. John Wiley & Sons.

Pitarch, J. L., Sala, A., & de Prada, C. (2019). A systematic grey-box modeling methodology via data reconciliation and SOS constrained regression. Processes, 7(3), 170.

Rahi, S. (2017). Research design and methods: A systematic review of research paradigms, sampling issues and instruments development. International Journal of Economics & Management Sciences, 6(2), 1-5.

Omito, O. (2016). Evaluating Learners's Ability to Use Technology in Distance Education: The Case of External Degree Programme of the University of Nairobi. Turkish Online Journal of Distance Education, 17(4), 147-157.

Romero, D., & Vernadat, F. (2016). Enterprise information systems state of the art: Past, present and future trends. Computers in Industry, 79, 3-13.

Ryan, G. (2018). Introduction to positivism, interpretivism and critical theory. Nurse researcher, 25(4), 41-49.

Sharma, S. K., Al-Badi, A. H., Govindaluri, S. M., & Al-Kharusi, M. H. (2016). Predicting motivators of cloud computing adoption: A developing country perspective. Computers

Safa, N. S., & Von Solms, R. (2016). An information security knowledge sharing model in
organizations. Computers in Human Behavior, 57, 442-451.

Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. International Journal of Information Management, 36(2), 215-225.

Sumra, I. A., Hasbullah, H. B., & AbManan, J. L. B. (2015). Attacks on security goals (confidentiality, integrity, availability) in VANET: a survey. In Vehicular Ad-Hoc Networks for Smart Cities (pp. 51-61). Springer, Singapore.

Tiffany, D., Cole, C., Joanna, L.(2019) Elevating cybersecurity on the higher education leadership agenda. https://www2.deloitte.com/insights/us/en/industry/public-sector/cybersecurity-on-higher-education-leadership-agenda.html

Wagdy Sawahel 22 September 2017: Universities face an age of cyber crime: https://www.universityworldnews.com/post.php?story=2017092208032052

Wara, Y. M., & Singh, D. (2015). A guide to establishing computer security incident response team (CSIRT) for national research and education network (NREN). African Journal of Computing & ICT, 8(2), 1-8.

Yaokumah, W. (2017). Modeling the Impact of Administrative Access Controls on Technical Access Control Measures. Information Resources Management Journal (IRMJ), 30(4), 53-70.

Yau, H., (2014) Information Security Controls. Advances in Robotics. [online] as accessed on 20/8/2019 https://www.omicsonline.org/open-access/information-security-controls-2168-9695.1000e118.php?aid=23716