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

http://www.ijssit.com

ICT PERSONNEL TRAINING FOR IMPROVING DATA SECURITY, ACCESS CONTROL & SYSTEMS MONITORING

[1*] **Charles Ochieng' Oguk**
Rongo University
Email: ogukcharles@gmail.com

Abstract

The study determined the effects of ICT personnel training on access control & systems monitoring within public Universities in Kenyan. Hacking information systems has been in the rise in Kenya, wherein breaches of data security and unauthorized access have been witnessed. Findings by studies, among them, Deloitte Kenya Ltd indicated that East African business computer networks that contain organizational critical data, are still vulnerable to attack and fraud on the electronic platform. To reduce the problem of hacking computer networks, institutions conduct on job-Information Technology security training for I.T professionals. The uncertainty on effects of such training has led to a focused attention in on-job IT security Training and its effects on data security, access control & systems monitoring within public Universities in Kenyan, to analyze how the data/information security attributes is affected by the training. The specific objectives have been; to investigate the effects of ICT personnel training on the management of access control as well as monitoring; to determine the effects of ICT personnel training on data security management. From 31 public Universities in Kenya, with network related personnel population of 409 ICT, a sampling formula was employed that yielded a sample size of 203 personnel. Random sampling was done, thereby administering questionnaires to the sample for data collection. Data has been analyzed using correration and regression model in Tobin's Q equation in conjuction with Likert model. The major outcome of the study was a positive correlation between the training and all the elements of computer network security management, thus determininhg the relationship under study. The findings could be significant to organizational policy makers, security trainers and IT heads in managing University network security more effectively.

Keywords: *ICT personnel, Data security, access control and monitoring*

INTRODUCTION

Background of the study

Globally and locally, universities have adopted the use of computer data networks to boost their business performance. Kelechi, (2003) found that without data, companies would be lost, not have a way to operate, causing businesses to operate slower. Apart from providing access to centrally stored data / information, and ease of sharing these resources, computer data networks offer speedy connectivity and ultimate value to businesses (Kelechi, 2003). Despite the importance of computer data networks, there have been numerous reports of information security concerns and high magnitudes of resultant losses from breaches. Jackson,

(2013), noted that almost on daily basis, we get informed by the media of an internal information systems security breach somewhere as Cyber burglars are constantly getting new ways to penetrate even the most complicated firewalls and security systems. Hacking communication channels seems to be a daily occurrence in Kenya (Standard digital: Saturday 26th October 2013). The Kenyan electoral body, IEBC database system was attacked by 'red-October' virus (Kenya Daily Express, Thursday, 7 March 2013). There was report that Kenyan institutions' computer networks are attacked due to poor data security, resulting in big losses (Business Daily: Monday, June 11 2012). Recently, the Kenya judiciary information systems channel was reportedly invaded (Standard digital, October 16, 2013). Nacht, (2011) notes that Security administrators constantly live in the fear of getting a late night call of IT network systems being invaded by hackers. The time between vulnerability and exploit is quickly shrinking, and in mostly exploits spread before many organizations can apply appropriate vendor remedies, (Nacht, 2011).

To complicate matters, some of the most insidious attacks are those that are not reported, hence don't make the headlines - internal hacking, electronic extortion, and other attacks targeted at specific organizations for financial gain or retaliation are occurring more frequently, (Nacht,2011). Findings by Deloitte Kenya Ltd indicated that East African business Information System are vulnerable to attack, fraud and confidentiality breaches, with insiders posing a bigger security threats than outsiders (Deloitte, 2011). Computer data security issue is so conspicuous that it has attracted attention of many IT researchers. Naeldecosta, (2013), noted that information security is important for every organization whether small or large for monitoring of employees and information resources therein. It is important that companies make significant investment in network security in order to protect its proprietary data from hackers and other criminals (Donald, 2012). The trend of compromising institutional computer systems has been so much that Kenyan Government has embarked crackdown on cybercrime (Daily Nation: September, 21 2013). The government of Kenya launched a blueprint to prevent cybercrime in the year 2011 (Daily Nation, November 21, 2011).

Statement of the Problem

ICT security training should impart skills for better protection of organizational data confidentiality, integrity and availability, there has been, however, a discourse on the possible effects that imparting such skills to IT personnel could have on data security, access control and systems monitoring. While some perceive the training to bring forth positive returns, others feel it may expose the internal IT systems to even more risks. Acry and Hovay (2008) found in their study, that most system security incidences originate from within an organizations. The problem is that while the effects of ICT security training on institutional data security remains unclear, managers continually invest on IT security training. In spite of this apparent uncertainty, there is hardly any research work directed to data security, access control as well as system security monitoring, to analyze how they are affected by the on-job IT security training. A closer review of existing related studies indicate that they hardly focused on this subject, hence the need for this study.

Purpose of the Study

The main objective of the study was to investigate the effects of ICT personnel training on- access control & systems monitoring within universities in Kenya.

Specific Objectives

The study was be guided by the following specific objectives,

i) To investigate the relationship between ICT personnel training and data security management.

ii) To determine the relationship between ICT personnel training and management of network access control & monitoring

Research Questions

i. What is the level of relationship between ICT personnel training and network data security management?

ii. What is the relationship between ICT personnel training and management of network access control & monitoring?

Significance of the Study

The study is significant as its findings has put into perspective the effects of ICT personnel training on institutional data security. This could be of benefit to organizational heads, ICT managers and IT training institutions. It could assist organizational heads in justifying approvals for expenditure in support of IT security training for their I.T professionals. The study may help ICT mangers to model an ideal secure ICT infrastructure, improving on network security tools. Specifically, ICT managers may use the study findings to secure increased budget for IT security training.

Scope of the Study

The study sought to investigate theeffects of ICT personnel training on the institutional data security, system access control and monitoring. The study focused on establishing the relationship / association and the strength of association between the training and each element of data security. It was conducted within the ICT departments of the sampled Kenyan public Universities, and targeted only the technical staff members.

Limitations of the Study

The researcher was confined within the realms of IT security training and network security. The study also encountered unwillingness by some respondents to reveal information, which was classified as confidential. However, the researcher assured the respondents that the data collected and the findings would be held confidential and used for academic purpose only. To further assure the respondents of confidentiality, names of institutions were not shown and also, the identities of the respondents were not being required. These made the respondents more comfortable to fill in the questionnaires.

LITERATURE REVIEW

Elements of data and information security

ICT infrastructure with unstable or insecure data/information systems hardly supports organizations' core business and is also vulnerable to attack. Daya (2009), and Mullard, (2007), identified the following as vital aims of computer information security; increase accessibility of resources to authorized entities, data confidentiality, system authentication, data integrity, non-repudiation, availability and privacy. Mullard, (2007) notes that data security in a network deals specifically with regular vulnerability assessment, access control, security policy, resource availability, user management, data security controls, monitoring / detection, software patches / updates.

To reduce network vulnerability attack, training is one approach of mitigation adopted by most institutions, especially the Kenyan public Universities, to enhance network security. Indeed, Kenya public Universities spend heavily to build employee capacity through on-job training. Most HR professionals agree that employee training is a complex human resource practice that can significantly impact a company's success ((BRUM, 2007). Knapp (2005), in his research concluded that user training has a very strong relationship with information systems security management effectiveness. In Kenya, Universities and other institutions offer on job IT security training to their employees – the I.T professionals, in attempts to ensure effective use of IT security tools and improvement of the network security. NIST, (1998), indicated that in a highly networked computer environment, an institution cannot protect the integrity, confidentiality and availability of information without ensuring that each worker is adequately trained on the subject.

Anderson (2007), found that in IT infrastructure, well-trained teams perform demonstrably better than under-skilled teams and that performance results in measurable improvement in productivity. In his research work, Anderson showed that teams that are well trained in information security and availability disciplines were 10% more productive and accounted for $70,000 worth of improvement annually. IT organizations that believe that the talent of their teams can keep up with the change in technology without actively developing skills risk poor performance and failed investments (Anderson, 2007). Statistics indicate that investment in training is continuing to grow as more and more companies, Universities and other institutions realize the importance of training. Institutions invest heavily in training IT personnel on IT security as there are both direct and indirect expenses involved. In 1995, $7.7 billion was spent on the wages and salaries of in-house company trainers and $2.8 billion was spent on tuition reimbursement (Frazis, et al., 1998).

Kenyan Universities also spend a big percentage of their budget in training IT personnel on IT security. As such, it is imperative for institutions to understand the effects of on-job IT security training on their institutional network, particularly network security management. Kaufman & Hotchkiss, (2006), concluded that in general, a company will weigh the costs and returns of training to determine the amount of investment it will incur. But does on- job IT security training has any effect on the institutional computer network security management? Since Kenyan institutional managers regularly incur high investment expenses to provide IT security trainings to their I.T professionals, the managers and other stakeholders really need to adequately comprehend the effects of on job IT security trainings on the computer network security management within their organizations (researcher).

ICT Security Training and Data Security

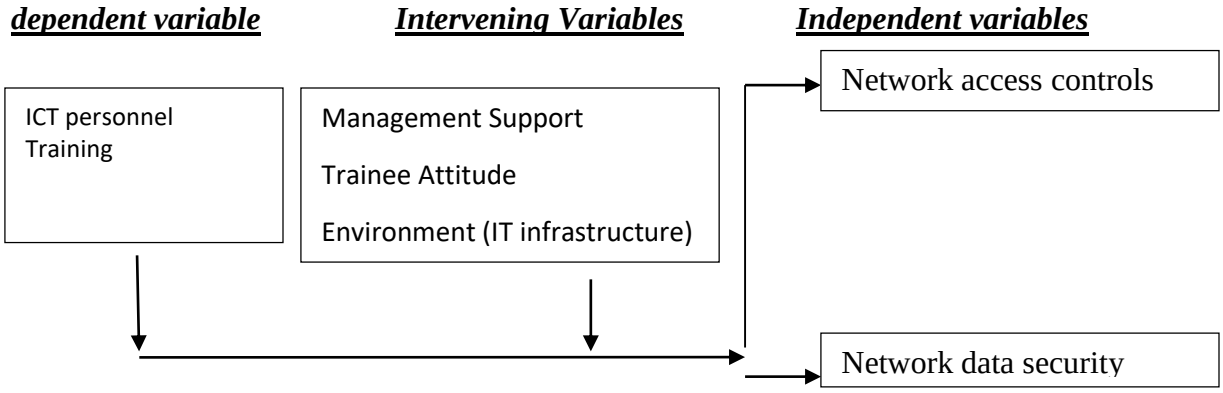
Denning (2012), in a research study, explored some of the attack tools practically used by network attackers. It revealed that the attack techniques are used by criminals to analyze signals getting into and out of a network. It showed that criminals penetrate network defense mechanisms like the firewalls thus accessing the institutional networks unlawfully. While inside the network, the attack technologies bypass detection intelligence offered by intruder detection / prevention systems, thus interfering with the institutional network monitoring systems. According to the study, the attack techniques actually make computer networks highly vulnerable for data loss, penetration, network auditing / monitoring, and integrity & confidentiality breaches. The study concluded that continuous training of employees on IT security is recommended, thus creating a grey area, prompting the need of a research to establish the relationship between the on-job IT security training and network access control / monitoring.

Impacts of On-Job Training on Performance

Trust – KENET, and other institutions, conduct on-job IT security training each year to the IT employees from different Kenyan Universities and other institutions of higher learning, (researcher). The training is conducted at a quite high cost, and indeed most of the public Universities set aside millions of shilling for training every financial year, (researcher). Training can have a considerable influence on company finances as there are several potential training costs that companies may incur. One type of training related cost is direct cost. This may include instructor salary, materials, and follow-up supervision. A second type of training related cost is indirect cost. These costs are related to worker output and productivity during and upon completion of the training, (Brum 2007).

Companies can seek to achieve organizational goals through a variety of human resource strategies and approaches. One such approach, a commitment strategy, attempts to develop psychological connections between the company and employee as a means of achieving goals. Patrick Owens (2006), while trying to determine employee - employer psychological connection through on-job training had a similar finding. In his study, Owen centered on the overall impact of training and organizational outcomes. By applying the results of his survey to independent t-tests, Owen was able to determine that trained employees had organizational commitment of 83.54, while the untrained employees had 75.87 for commitment to employer. By separating the trained and untrained employees, Owen was able to show that an employer may improve commitment levels of employees through training, thus increasing employee performance as well. This argument is supported further by researchers, (Walton, 1985), who showed that more committed employees will perform much better at their jobs. Also, Brum (2007), indicating that commitment has a significant and positive impact on job performance.

Conceptual Framework



Source: Author (2018)

RESEARCH METHODOLOGY

Target Population

The target population for the proposed study included all the 409 database related staff members from ICT departments of all public Universities based in Kenya.

Sample Size

According to (Yamane, 1967), the sample size (n) for the study is given by;

$$n = \frac{N}{1 + N e^2}$$

$$n = \frac{409}{1 + 409\ (0.05)^2}$$

$$n = 203$$

Where n= sample size, N= population size and e= the error of five percentage points. The target sample size being 203 respondents. The total numbers of respondents who successfully filled and returned the questionnaire were 150

Data Collection instruments

Questionnaire tool was found approriate after piloting as it would help collect as much data as the researcher wanted, and at the comfort of the respondents.

Regression model

Sub-elements of data security were quantified using a Likert scale scores whose means were computed for all factors (sub-elements) within the main element of network security. Regression model was used as:

$Qt = \beta_0 + \beta_1 DS + \beta_2 AM$ (modified Tobin's equation)

Whereby β_0 is constant of the model while β_1 and β_2, are the coefficients of the dependent variables

Qt = Tobin's Q of the on-job IT security training as the dependent unit in a public University.

DS = Total mean scores for the Data security. Most empirical studies support the view that data security deals specifically with CIA. That is, data Confidentiality, Integrity and Availability. Data security as one of the main elements of network security has sub-elements or factors like; data encryption, application availability, back-up, archival and restoration

AM = Total mean scores for the Access control and monitoring. This has sub elements like control of both internal and external access, monitoring and understanding of therein tools.

DATA COMPILATION, ANALYSIS AND PRESENTATION

Table 1: Access control from external networks

Performance levels	**Percent**
Very ineffective	15.3
Ineffective	20.0
Moderately effective	29.3
Effective	24.0
Very effective	11.3
Total	**100.0**

As shown, levels of controlling access from entrusted external networks to the trusted University network is a key indicator of network security management within the University network. Without this, there is uncontrolled entry, which comes along with vulnerability to malware attack, lack of data integrity, resource misuse, among many vices. Responding to this, a majority of the respondents, 29.3 % of the sample, indicated moderate effectiveness of control measures applied against access from external networks. 24 percent of the respondents showed that it is effective, while only 11.3 percent indicated that the measures being employed are very effective. However, about 36 percent of respondents indicated that the control measures are not effective in their institutions.

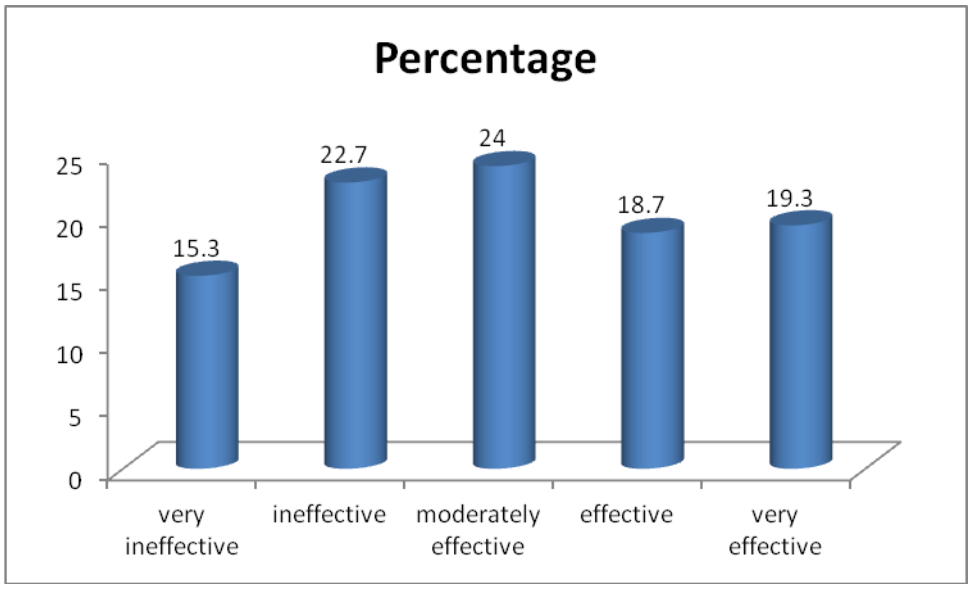


Figure 1 Access control from initial networks

Results similar to external access case were depicted when internal network access control measures in different Universities were considered, as shown in figure 1. Only 19 percent of the respondents accepted that there are very effective levels of access control within their internal networks. Moderately effective was at 24 percent, while a total of 40 percent showed that internal access control measures were ineffective in their Universities.

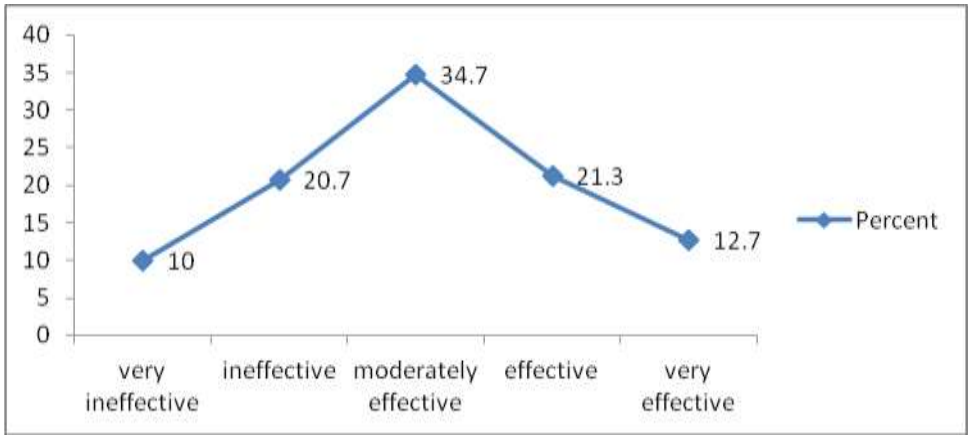


Figure 2: Use of IT systems for risk monitoring

Using automated tools to monitor network for any risk is very important, as it helps to detect and isolate threats in advance, hence rescuing resources which could be vulnerable. The monitoring tools are mainly the IDS/IPS – intruder detection systems and also intruder prevention systems which come as appliance containing IDS embedded therein. This question would as well be an indicator of the availability of monitoring tools as installed in the network systems. As shown in the figure 2 above, 34.7 percent of the respondents indicated that they moderately use IT systems effectively to monitor risks within their network infrastructure. 12.7 percent of those sampled use the tools very effectively, while 10 percent and 20.7 percent indicated very ineffective and ineffective use respectively, of such monitoring tools.

Levels of understanding data network management tools

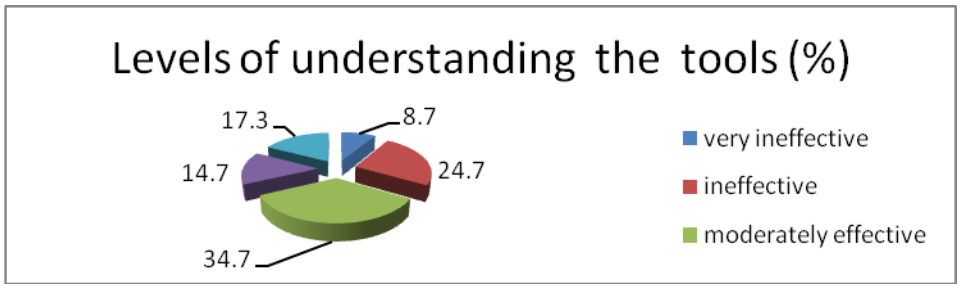


Figure 3 understanding freeware data network managing tools

As nature dictates, there is always scarcity of vital resources, where institutions struggle with budgets to fund their ICT infrastructure. ICT personnel resort to freeware with equivalent effectiveness just as the commercial products, to safeguard their networks amidst resource scarcity. The freeware has assisted in effective network security management despite scarce resources. It would be expected therefore, that those who have been trained should be aware of most of the listed network security management tools and their areas of applicability.

According to figure 3 above, most respondents, 34.7% indicated moderate understanding of the tools, while 8.7 percent showed minimal understanding of the same.

Element two: Network data security (CIA)

Network data security is mainly concerned with Confidentiality, Integrity and Availability of data, either in stored files or from applications in use. Confidentiality implies limiting data access to only authorized persons. This means that, while an intruder may break through network defense firewalls and actually penetrate the network, user applications and data therein should still be safe if confidentiality is upheld within the network. Data integrity implies restricting alteration of data to only authorized personnel. Data availability requires that access, retrieval and restoration system for data are efficient and timely enough, to present data to the user at optimal operation levels. The figures below indicate responses from the sampled respondents, regarding various factors (sub-elements) of network data security.

Levels of data encryption

Organizations which value their data use network security technologies like encryption, digital certificates, SSL, and/or other similar technologies to secure electronic files, centrally held data, and data in online transit. To further ensure data security, empirical results from earlier studies indicate that control of sneaker–net is desirable.

Table 2 Levels of data encryption

Performance levels	Percent
very ineffective	20.0
Ineffective	25.3
moderately effective	17.3
Effective	16.0
very effective	21.3
Total	**100.0**

From table 2 above, majority of the respondents, at 25 percent showed that data encryption was ineffective in their Universities, while only 16 percent showed that it was effective. 17.3 percent of the respondents showed that data encryption was moderately effective in their Universities. Analyzing the responses, more than 45 percent of the respondents showed that encryption was ineffective in their institutions. This could be caused by either lack of encryption tools within the network, or incompetence by the personnel to effectively apply the available data encryption tools.

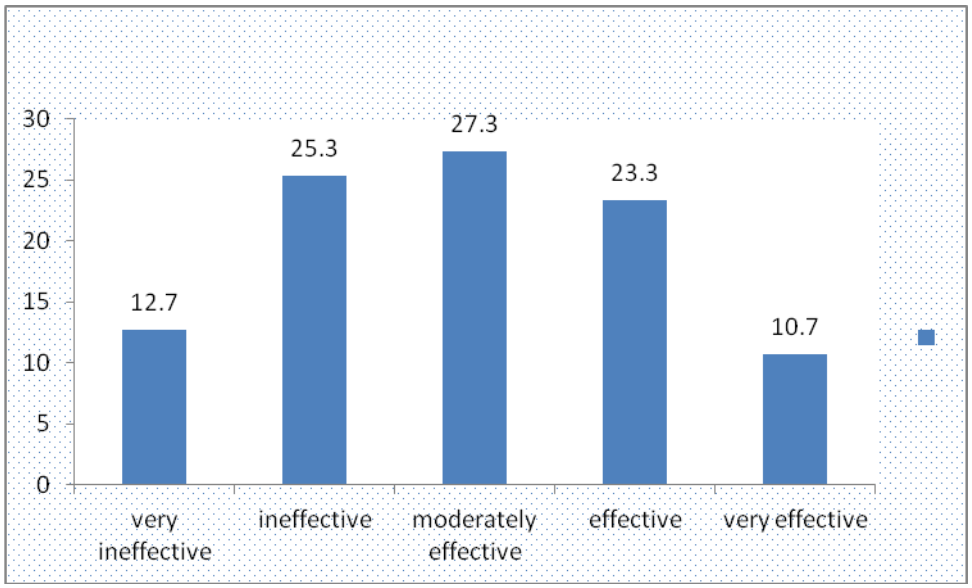


Figure 4 Levels of sneaker-net control

Sneaker net is the transfer of electronic data and or information, especially computer files, by physically moving removable media e.g. USB flash-disks or external hard disks from one computer system to another. It would therefore be expected that workers who are trained could keep their networks more secure by avoiding the use of sneaker nets. According to figure 7 above, there is moderately effective control of sneaker – net at 27.3 percent as reported by the University IT personnel sampled. 23.3 percent reported effective control, 10.7 percent very effective, 25.3 percent ineffective, while 12.7 percent reported very ineffective. Data retrieval form archival locations are considered effective if they are achievable within one hour. More efficient data back-ups are achieved easily when centralized server back – ups are employed successful data back-ups.

Table 3: Levels of successful data back-ups

Levels of successful data back-ups	Percentage
Very Ineffective	18.0
Ineffective	24.0
Moderately Effective	20.0
Effective	22.7
Very Effective	15.3
Total	**100.0**

Successful data back-up entails regularly saving user data, both at primary and secondary levels. With regular data back-ups, should the volatile data be lost during operations, it can still be found within the primary storage facilities. Both primary and secondary storage ensure network data availability at the optimum operation levels, thus contributing to the "A = availability" in CIA of data security. Table 11 indicates that 18 percent of the respondents indicated very ineffective data back-up in their Universities, 24.0 percent indicating ineffective, 20 percent moderately effective, 22.7 percent effective and 15.3 percent very effective successful data back-up.

Data Restoration

When computing operations are interrupted in an organization, analysts consider the period taken for complete restoration, which in this research was pegged at 24 hours, universal figure for maximum. This means that however much the interruptions could be, at least full operation should be restored within 24 hours.

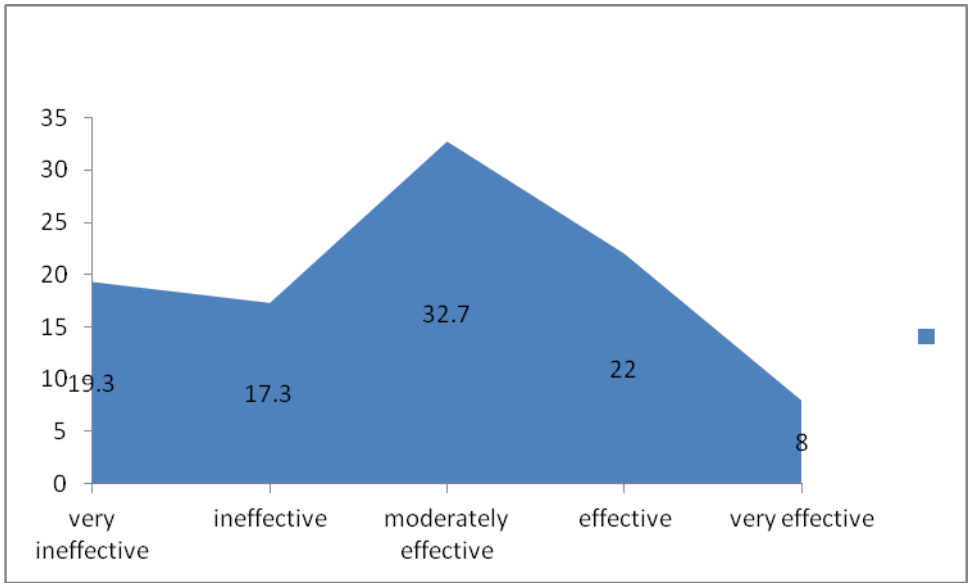


Figure 5: Levels of successful restoration within 24 hours

According to figure 5 above, 32.7 percent of respondents indicated that data restoration within 24 hours is achieved at moderate levels within their Universities. 19.3 percent showed that the restoration was very ineffective, while only 8 percent reported very successful restoration.

Table 4: Levels at which centralized server back-ups are deployed

Responses	Percentage
Very ineffective	8.0
Ineffective	13.3
Moderately effective	36.7
Effective	21.3
Very effective	20.7
Total	**100.0**

Table 5: Availability levels of critical servers and applications

Responses	Percentage
Very Ineffective	5.3
Ineffective	14.0
Moderately Effective	28.7
Effective	40.7
Very Effective	11.3
Total	**100.0**

Availability of critical servers and applications for users in a University network is a vital aspect of data security. Table above shows that 40.7 percent of the respondents reported that it was effective, 28.7 percent moderately effective, 14.0 percent ineffective, 5.3 percent very ineffective, while 11.3 percent of the respondents showed that it was very effective.

Table 6 Levels of Successful archive retrievals within 1 hour

Response	Percentage
Very ineffective	8.7
Ineffective	11.3
Moderately effective	25.3
Effective	42.0
Very effective	12.7
Total	**100.0**

Data availability principal requires that data in the archive when needed should be retrieved promptly, usually within an hour. 42.0 percent of the respondents indicated that retrievals are effective in their Universities, 12.7 percent, very effective, 25.3 percent moderately effective, 11.3 percent ineffective, while 8.7 percent of the respondents indicated that archive retrievals were very ineffective within their domains. Thesis summarized in table 8 above.

Correlations and Regression Analyses

Relationship between On–job IT Security Training and Network access control & monitoring

Model elements	Pearson correlation	Sig.
access control from external networks	.704**	.000
access control through internal networks	740**	.000
use of IT systems for risk monitoring	.272**	.001

Levels of data encryption	.741**	.000
levels of sneaker-net control	.270**	.000
successful data back-ups	.764**	.000
Unsuccessful restoration within 24 hours	-.813**	.000
Availability of critical servers and applications	.428**	.000
successful archive retrievals within 1 hour	.385**	.000

Regression analyses

Regression model was used as:

$Qt = \beta_0 + \beta_1 DS + \beta_2 AM$ (Tobin's Equation)

Model elements	**Unstandardized Coefficients**		**Standardized Coefficients**	**t**	**Sig.**
	B	**Standard error**	**Std. Error**		
(Constant)	1.992	0.149		0.369	0.000
Access cont.&Monit	1.62	1.84	0.791	0.880	0.023
Data Security	0.80	0.53	0.391	1.509	0.030

As shown above, the correlation coefficient values of +0.704 and +0.740 indicate a strong relationship between on-job IT security training and control of network access from external (un-trusted) and internal networks respectively. This implies that with more training, techies acquire more skills and adopt technologies for controlling access to, and within their networks. A correlation coefficient value of (+0.272) in table above points to a weak positive linear relationship between on-job IT security training and deployment of IT systems to monitor risks / threats within a network. This means that so much increase in such training units results in only little increase in the deployment of such threat monitoring units within Kenyan public Universities' computer networks.

Table above shows a correlation coefficient value of (+ 0.741), indicating a strong positive linear relationship between on-job IT security Training and levels of data encryption within the University networks.The r value of (+0.270) and (+0.282) in table above and d below show weak positive relationships between the training and levels of sneaker – net control, and between training and successful restoration within 24 hours.

There is a strong positive relationship between the training and successful data back-up, with an r value of (+0.764).

There is a strong positive relationship between the training and successful restoration within 17 hours, as shown in above. A more interesting value was noted in table above, where the correlation coefficient value is (-0.813). This means a strong negative relationship between on-job IT security training and Unsuccessful data restoration within 24 hours. This implies that more training conducted results into more successful data restorations. A relationship similar to table seen in table above, which indicates a correlation coefficient value of (-0.642) between the training and unsuccessful archive retrievals within one hour. This means that as the Universities increase on-job IT security Training, the unsuccessful cases of archive retrieval reduces. Tables above reveal a moderately positive relationship between on-job IT security training and; Regular centralized server back-ups, Availability of critical servers and applications, and successful archive retrievals within 1 hour.

The average r value for Network data security is obtained by adopting absolute values on-job IT security and each factor of network data security: |(0.741+ 0.270+0.764 + 0.282+ 0.813+ 0.642 + 0.437 + 0.428 + 0.385)| / 9 = +0.529. The correlation coefficient value of +0.529, as seen between on-job IT security training and Network data security - as an element of network security, indicates a positive moderate linear relationship between the two variables. Information in tables above was used towards generating the coefficients / factors necessary for completing the Tobin's equation, relating the element (access control and monitoring) and on-job IT security training. Thus: **Qt = 4.979 + 2.132 DS + 1.992 AM**

Conclusions

The study found that on job IT security training improves data security management, access control and systems monitoring within Kenyan public Universities.

Recommendations

It is evident that on job IT security training has an influence on data security management in Kenyan public Universities. Hence, there is a need to strike a good balance between personnel training and data security appliances within IT departments

It is recommended that organizational heads should approve appropriate budgets in support of IT security training for their I.T professionals, as the training will help manage their data and general information systems security better.

REFERENCES

Anderson, C., (2007). Information security and availability: The Impact of Training on IT Organizational performance. Retrieved from www.idc.com.

Deloitte., (2005). Global Security Survey. New York.

Denning, D., (1986). An intrusion detection system: proc. Symp. Security and privacy, IEEE Computer Soc. Press, Los Alamitos, Calif. pp. 118–131.

Frazis, H., Gittleman, M., Horrigan, M., & Joyce, M., (1998). Results from the 1995 Survey of Employer Provided Training. Monthly Labor Review, 121(6), pp. 3-13

Kirkpatrick, D. L., (1976). Evaluation of training, Training and development handbook, A guide to human resource development, New York; McGraw-Hill Company.

Kaufman, B., & Hotchkiss, J., (2006). Economics of Labor Markets (7th ed.). Mason, OH Thomson South-Western.

Mullard, S., (2007). Network security: the impact of computer and network security in corporations today. http://ttcshelbyville.files.wordpress.com/networksecurity.doc.

Walton, R. E., (1985). From control to commitment in the work-place. Harvard Business Review, 63(2), pp. 77-84.

Yamane, T., (1967). Statistics: An Introductory Analysis, (2nd Ed). New York: Harper and Row.

Yang, T. A., (2001). Computer security and impact on computer science education. [available at sce.uhcl.edu/yang/research/Computer Security/ccscne2001.htm]