IMPACTS OF ICT SECURITY TRAINING ON MALWARE CONTROL AND POLICY IMPLEMENTATION IN UNIVERSITIES' COMPUTER NETWORKS.

Charles Ochieng' Oguk
coguk@rongovarsity.ac.ke, ogukcharles@gmail.com
ICT Department, RONGO UNIVERSITY.

ABSTRACT

The study determined the effects of ICT personnel training on malware control and security implementation within public Universities in Kenyan. Malware infestation and unauthorized practices in information systems have been in the rise in Kenyan universities, thereby compromising integrity of critical information therein. studies indicate that malware causes breaches of data integrity and availability. While universities and other institutions conduct employee security training in order to lessen the impact of such information systems' security breaches, the effectiveness of such trainings with respect to security elements have not been established. The desire to assess the real effects of such training on the intended purpose has led to a focused attention in ICT security Training and its effects on malware control and implementation of security policies within public Universities in Kenyan. The study objectives have been; to investigate the effects of ICT personnel training on malware control ; to determine the effects of ICT personnel training on implementation of security policies in computer networks within universities in Kenya. Out of 31 public Universities in Kenya, with a population of 409 network related personnel, a sampling formula was employed that yielded 203 personnel as a sample. Questionnaires were administered to the sample for data collection. Data analysis was mainly through correration and regression model in Tobin's Q equation in relation to Likert model. The major outcome of the study was a positive correlation between ICT security training and all the features of malware control and security policy. The findings could be significant ICT managers for boosting IT security management.

Key word: ICT personnel, IT security training, malware control, policy implementation

INTRODUCTION

Apelu (2007) defined computer network as a group of computers interconnected to facilitate sharing of information and other computer based resources. Kelechi, (2003) found networks facilitate way to communicate hence enhancing businesses operations through according access to central databases and speedy internet connectivity. Besides this, the networks allow the user to access remotely located resources like databases regardless of the existing geographical distances, (2001, ICT Global, Inc.). Despite the levels of importance that studies allude to

computer networks, there exist many reports of malware and poor implementation of security policies as factors related to information security breaches and high magnitudes of resultant losses (Jackson, 2013). Hacking information systems of universities seems to be a daily occurrence in Kenya (Standard digital: Saturday 26th October 2013). Government institutions are not spared either. The electoral body - IEBC system was attacked by 'red-October' virus (Kenya Daily Express, Thursday, 7 March 2013), therby compromising the information integrity. Kenya judiciary communication network channel was reportedly invaded (Standard digital, October 16, 2013), and information confidentiality compromised. Nacht, (2011) expressed fears held by ICT Security administrators of high possibilities of their IT network systems being invaded by malware and hackers.

Statement of the Problem

ICT security training is widely understood as an approach meant to equip information technology professionals with high level skills for enhancing security of IT infrastructure. There has, however, been a uncertainty on the possible effects that such trainings could have on information system security. While the effects of on-job ICT security training on institutional malware management and security policy implementation remain unclear, the status quo withstands. However, there is hardly any research work directed to malware management as well as security policy implementation, to analyze how they are affected by ICT security training. The existing related studies hardly focused on ICT security training's impacts on malware control and policy implementation, hence the need for this study.

Objectives:

i) To determine the relationship between on-job IT security training and management of network malware.
ii) To determine the relationship between on-job IT security training and network security policy.

LITERATURE REVIEW

Owens (2006) succinctly expressed malware as malicious software, that brings harm to a computer and general information system and are usually in the form of viruses, worms, trojans, adware, spyware and rootkits, among others; with adversse effects of stealing protected data / information, deleting documents and could also engage / activate a software not approved by a user.Russell, (2002) conducted studies on IT security awareness training as a way of implementing an effective IT security strategy. The study, focused mainly on the insiders as the weakest security link, as they interact with the IT infrastructure, hardware and networks, thus posing a high risk of malware spread that occasion data integrity breaches and unavailability to

authorized users. The study found that on-job IT security training is vital for I.T professionals and users alike, and captured.

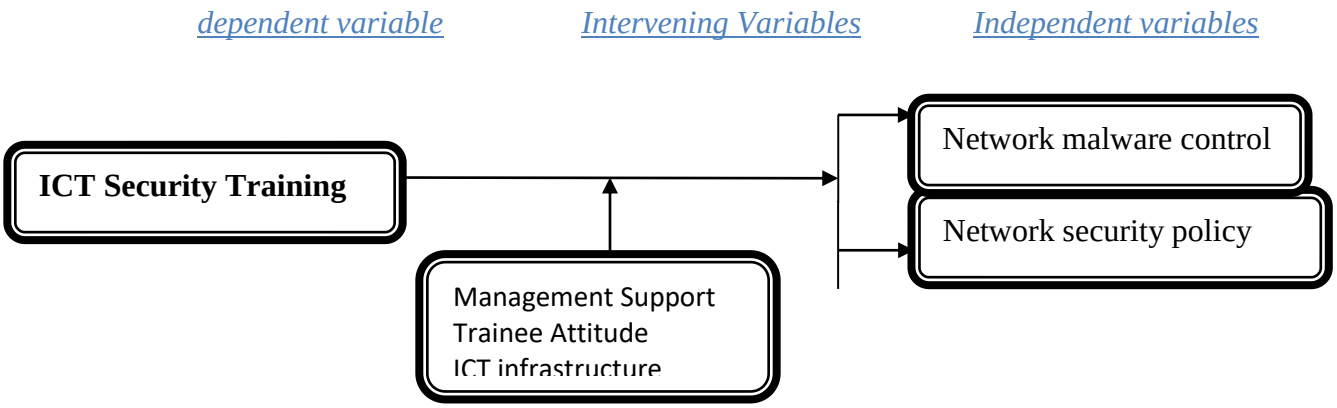
Mullard (2007) explained a network security policy as a management document that helps in protecting a network from related internal and external security. Daya (2002) broadened the discourse and showed that a network security policy document contains; rules and legal procedures for accessing the network, rules on governance over Web / Internet access, adminstration and Implementation of security procedures as well as defining privileges and services/processes any user can perform or access on the network. IBM, (2008), research work stressed the importance of training on implementation cum adherence to security policy. Uniquely, this study stressed and pointed out to a possible relationship between on-job IT security training and use of network security policy, which is a vital component of network security management. The possibility of an interesting relationship was further suggested by (Powanda, 1999), between on-job IT security training and use of network security policy within an organization. Both the IBM, (2008) and the (Powanda, 1999) studies did not attempt to establish the actual relationship between such trainings and network security policy. The researcher found this relationship very important, and went ahead to explore it further – the policy issue, to establish the relationship between IT security training within Kenyan public Universities and network security policy. Haywood, (1992) showed that since management controls training programs through policy formulation, budgetary and adoption of ideas for implementation, it should be considered an arbitrating factor in this kind of study.

Anderson (2007) revolved around the impact of IT security training on general organizational IT performance. The study focused on developing skills of on-job IT personnel and compared productivity levels of the trained staff against the untrained staff. It further developed an average bench-making levels using the (IDC, 2007) average performance criterion. It used malware control, data back-up & recovery, endpoint security, high levels availability, archiving and client management as the key elements of IT performance. The findings indicated generally that IT security training for I.T professionals indeed improves organizational performance. According to Anderson, (2007), 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. In conclusion, Anderson stated that IT organizations which take it that the talent of their workers can keep abreast with the change in technology without actively improving workers' capacity risk poor performance and unsuccessful investments (Anderson, 2007). The researcher utilized this approach, particularly in research design, but focused on management of a single component of organizational IT infrastructure - network security, to find out the effects of IT security training on this vital area of IT's wide field.

A review of Theory of Reciprocity

After training, the employees may feel indebted to the employer, thus the theory of reciprocity, as shown by Barrett and O'Connell through a research study. Barrett and O'Connell (2001) argue that employees may view some human resource practices as a "gift". Training is one such practice that employees may view as a "gift". The result of this "gift" is that employees exert more effort, become more productive, and have a greater sense of debt to the organization. The "gift" also has the potential to make employees feel like "insiders" into the organization. An "insider" is likely to be more committed and devoted to the company. The idea of "gift" and "insider" parallels closely to the concept of reciprocity, (Barrett and O'Connell 2001). The principal of reciprocity receives much support from other researchers in similar fields. According to Scholl, (1981), the premise behind reciprocity is that an employee will help the organization, because the organization helped the employee. The saying "don't bite the hand that feeds you" seems to correlate to the theory of reciprocity. This holds that employees should not only help the company but should also not hurt it because it was the company that helped the employee, (Scholl, 1981). Through an analysis of the above pertinent theory, and literature research done previously covering the impacts of on-job training on performance, this paper sought to better understand and clarify the impact that on-job IT (Information Technology) security training has on institutional network security.

Conceptual Framework



Source: Author (2014)

The study is concerned with the relationship between IT security training and institutional Network security, amidst intervening factors like management support, trainee attitude, and institutional IT infrastructure. The study is to explore the relationship between on-job IT security training (independent variable) and network security elements management (dependent variables)Support from management is vital for the success of any on-job training within an organization. Birdi (2005) found that poor managerial support directly effects on-job training and

its intended purposes. Haywood, (1992) showed that since management controls training programs through policy formulation, budgetary and adoption of ideas for implementation, it should be considered an arbitrating factor in this kind of study. Open-minded management could create a favorable environment ready to accept new ideas for implementation (Fischer & Ronald, 2011). Has Linda & Mahyuddin (2009) found that lack of support from top management is the main factor which affects the training effectiveness. The study noted that If there will be less support from top management, there is less chance of effective training program

Considering trainee attitude, Noe (1986), noted that trainees will develop positive attitude if they believe that;(1) high effort will lead to high performance in training, (2) high performance in training will lead to high job performance and (3) high job performance is instrumental in obtaining desired outcomes and avoiding undesirable outcomes. The study recognizes trainee attitude as a paramount factor which affects not only learning during training, but also performance after training. Therefore, the effectiveness of on-job IT security training, and the resultant performance levels of the trainee is affected by the trainee attitude towards training itself. The sentiment is concurrent with research findings by other scholars. Zaciewski (2001), conducting a research study in hospital industry learnt that trainee's individual characteristics such as motivation, attitude, and basic ability, affect training and the potential success of that on-job training. Still on trainee attitude, Beigi & Shirmohammadi (2011) found that emotional training has significant impact on learning during on – job training and the resultant service quality, meaning there is a relationship between attitude and learning. Another researcher, Saks & Haccoun (2007) came to a similar conclusion after exploring the psychological states of trainees especially motivation, self-efficacy, perceived control and the realities of the organizational context, and how these factors affect on-job training outcomes. Tai (2006) research work also concluded that general trainee's attitude and self-efficacy partially arbitrates the relationship between on-job training and learning as well as training outcomes. It was therefore, in the view of the researcher, that trainee attitude is such an important factor affecting learning during training and the applicability of the acquired skills after training, that it should be considered an intervening factor for this study.

The employee work environment also affects successful on – job training in general. Burke & Baldwin (1999) dwelled upon the transfer of skills during training and application of acquired skills at work place. The study indicated that the two could be enhanced by using real-world organizational problems. The factor of trainees' work environment emerges here. This indicates that trainees from institutions where IT infrastructure is well developed are more likely to perform better in learning during on-job training and applying the skills afterwards at workplace. The researcher attributes this to higher frequency of network security challenges noticed within robust IT infrastructure compared to armature IT set-ups. Also, Birdi (2005) found that an unfavorable departmental climate could deter creativity after training hence impeding idea implementation. The training may be as relevant and as intensive as intended, but the trainee's

work environment like a basic IT systems, could prevent implementation of the ideas acquired during training. These may water down the intention of such training.

RESEARCH METHODOLOGY

Research Design : the study was survey based, both qualitative and quantitative in nature.

3.2 Target Population and sampling

The target population for the proposed study included all the 409 technical staff members from ICT departments of all public Universities based in Kenya. 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 5%..

Data Collection instruments

The primary data collected through the questionnaire was concerned with the elements of network security in the organization's ICT infrastructure, composed of network malware control and network security policy. The primary data collected through well designed questionnaires was presented in tables and charts and summarized using the descriptive statistics.

Data Analysis and Presentation

The data collected was edited, coded, classified and entered in SPSS software, version 20, so as to present it for data analysis in a systematic and clear way. The primary data on network security element collected through the questionnaire was then analysed using descriptive statistics such as measures of central tendency which was majorly the mean. Inferential statistics, majorly the bi-variate analyses; regression, and correlation was performed to potray the relationship being studied, where the functional form of regression model in Tobin's Q equation, in conjuction with Likert model, was used, to reveal the causal relationships between (Independent variable) and (dependent variables).

Regression model

Regression model was used as:

$Qt = \beta_0 + \beta_3 MC + \beta_4 SP$ (Tobin's equation). Whereby β_0 is constant of the model while β_3 and β_4 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. MC = Total mean scores for Malware control, which include control of all sorts of malicious software through anti-malware installation, proper configuration, use of licensed software, updates and patches. SP = Total mean scores for the Security policy, which guides actions to be taken in various situations regarding network security. This entails development and internalization of network security policy, conformity of the policy with recognized industry standards and the levels to which the policy controls workers behavior, ensures risk mitigation, disaster recovery and business continuity.

RESULTS AND DISCUSSION

Network malware control

Malware is a technical name for malicious software in a network. Control of malware in the network is vital to ensure network security in general. For example, Malware like spyware can expose vulnerable points in the network, thus making it easy for crackers to employ attack strategies, compromising network security. To put malware at bay, techies should take a number of actions including; ensuring secure configurations for both hardware and software around all the hosts in their network. They should ensure that there is always anti-malware in the network, and that it is covered by the configuration assessment tools, including updates. Moreover, they should ensure that operating systems and other software used in the network are genuine, licensed and have necessary security updates as well as patches. The responses regarding levels of malware control are summarized as shown below.

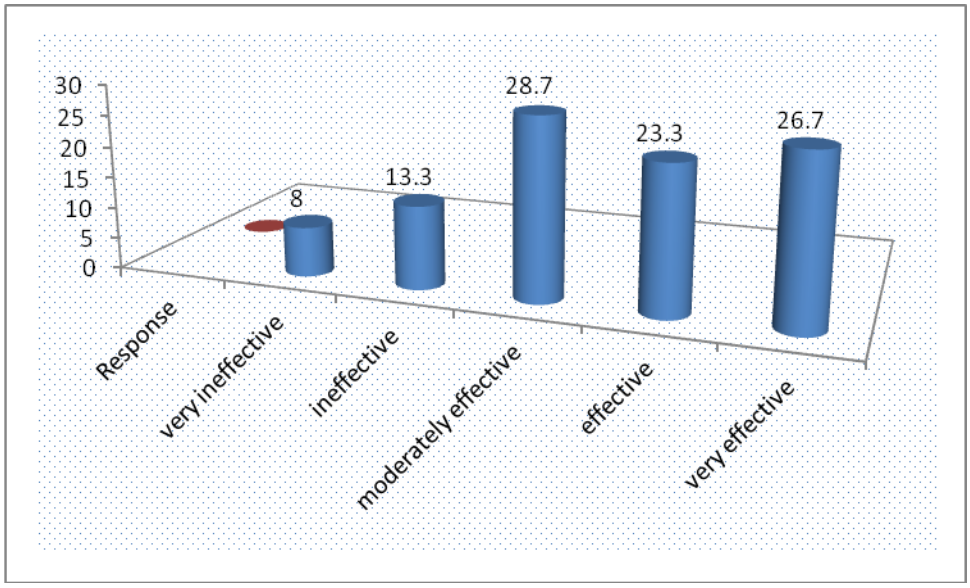


Figure 1: Levels of Secure Configurations for Hardware and Software

As seen in figure 1 above, most universities moderately employ secure configurations for their hardware and software. 23.3 percent showed it was effective, while 26.7 percent of the respondents showed that the practice was very effective within their universities. The figure 15

also shows that 13 .3 percent reported that the configuration practice was ineffective, while 8 percent showed that it was very ineffective.

Table 1: Levels to which Operating systems have security updates

Responses	**Percentage**
very ineffective	6.7
ineffective	23.3
moderately effective	17.3
effective	24.0
very effective	28.7
Total	**100.0**

Table 1 above summarized the respondents' responses in relation to operating systems' updates. It shows that the practice of updating OS was very ineffective among 6.7 percent, ineffective among 23.3 percent, moderately effective among 17.3 percent, effective among 24.0 percent and very effective among 28.7 percent of the respondents respectively.

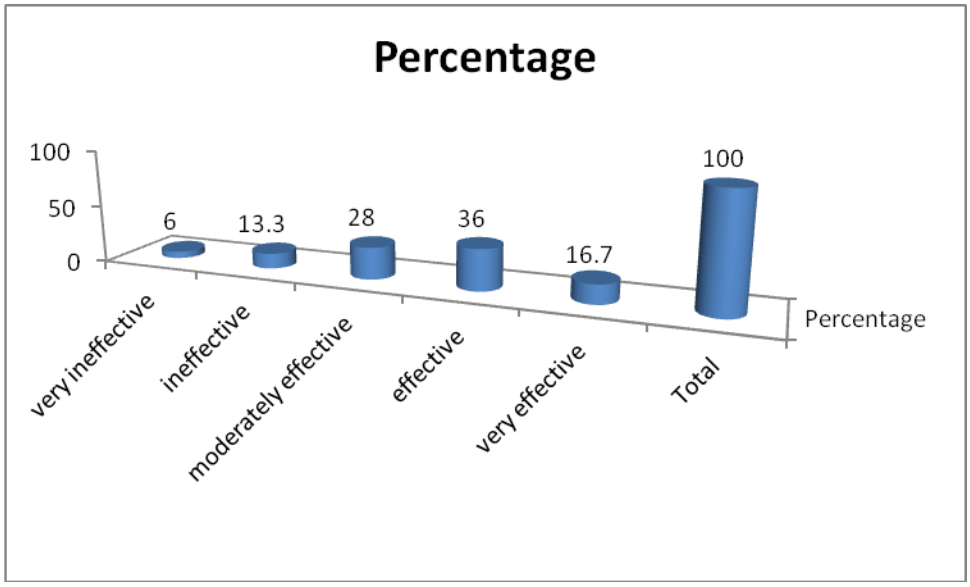


Figure 2: Levels to which Operating Systems and Application software are licensed

Figure 2 above shows that most Universities, at 28 percent moderately ensure that OS they use are genuine, 36 percent reported it was effective, while 16.7 percent showed that it was very effective. Only 13.3 percent and 6 percent of the respondents respectively indicated that it was ineffective and very ineffective respectively.

Element four: Network security policy

Where network security is prioritized, operations, actions and reactions of techies are normally guided by a formal document – the network security policy document. This document establishes the rules that guide the behavior of users and IT personnel when handling network information systems and the consequences for violating the IT security policy. In some organizations, the document is contained within a general ICT policy document. Organizations therefore, develop the network security policy and internalize it to effectively control operations within the network infrastructure. The network security policy is only effective, if it is developed on the foundations of recognized industry standards, legislations and regulations. It should enforce mandatory physical and logical access control to network resources and ensure risk mitigation, disaster recovery and business continuity in case of disaster. The effectiveness of the above elements associated with network security policy were investigated in this research, and responses were as shown below in tables / figures below.

Performance levels of Security Policy elements in different Universities.

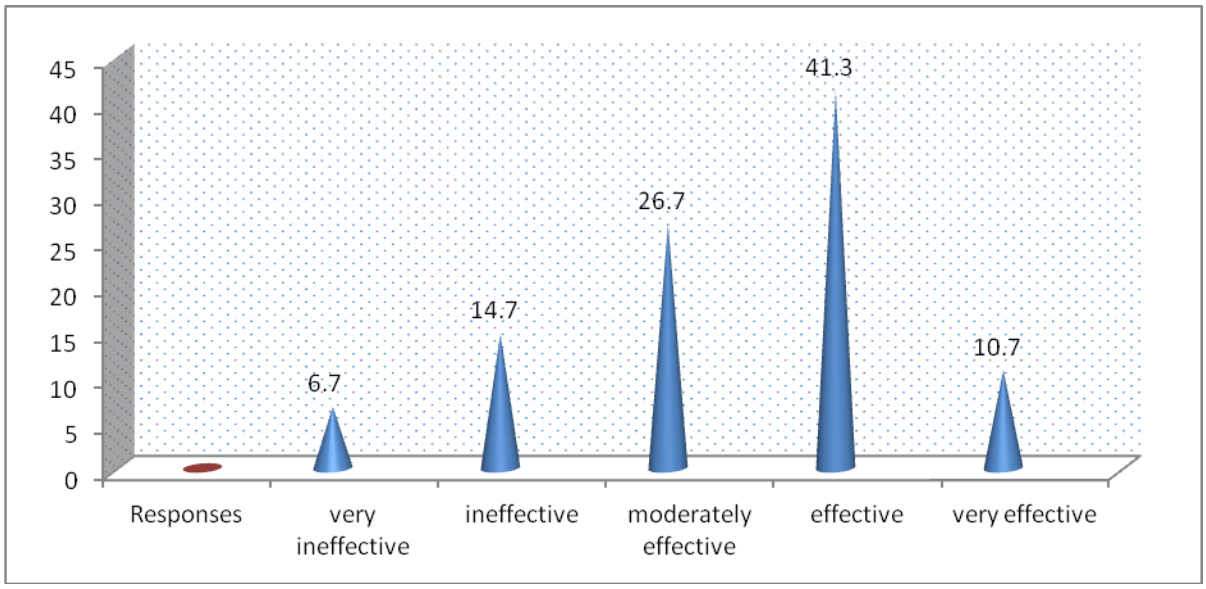


Figure 3: Network security Policy development and internalization within the organization

Figure 3 above shows that most respondents indicated that network security policy was developed and internalized within their Universities. This is because 26.7 percent showed it was moderately effective, effective at 41.3 percent and very effective at 10.7 percent. However, 14.7

percent and 6.7 percent respectively of the respondents showed that it was ineffective and very ineffective respectively.

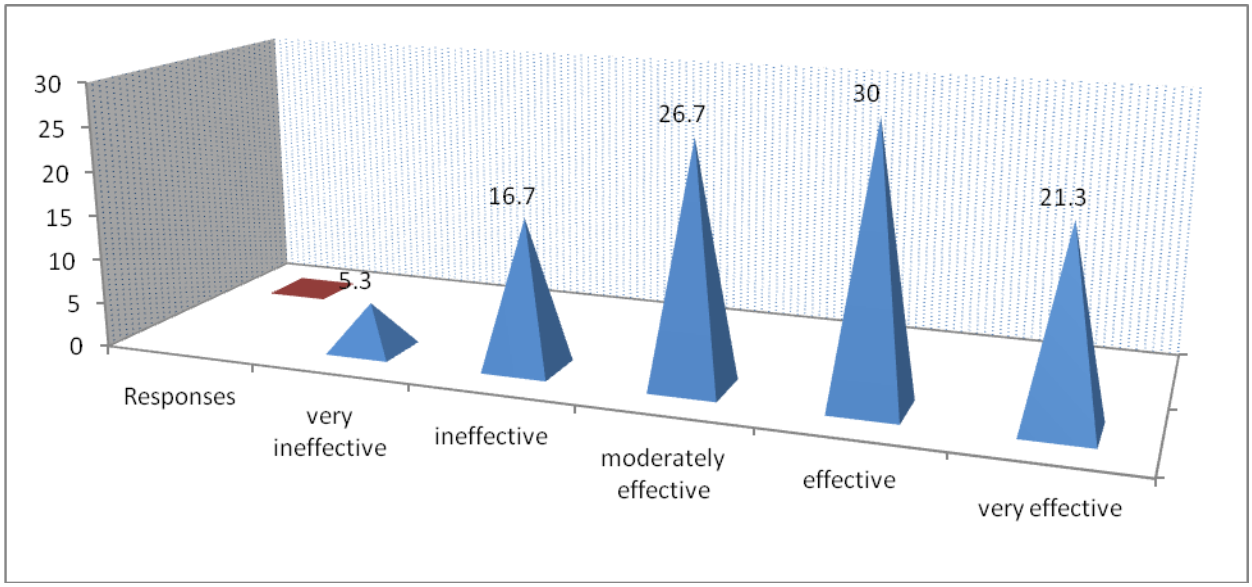


Figure 4: levels of Policy conformity to industry standards (in percentage)

As discussed earlier, a network security policy is more reliable when it conforms to well known and recognized industry standards and regulations. From figure 4 above, the conformity is seen to be 5.3 percent very ineffective, 16.7 percent ineffective, 26.7 percent moderately effective, 30 percent effective and 21.3 percent very effective.

Policy enforces mandatory access control

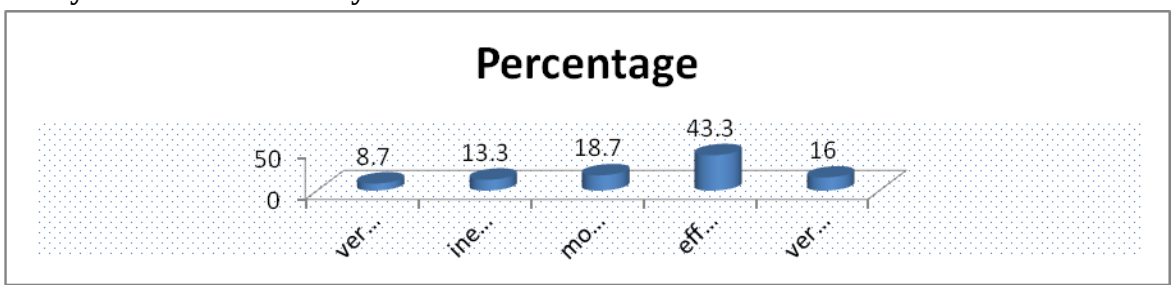


Figure 1 Levels to which the Policy enforces mandatory access control

Figure 5 above shows that in enforcing mandatory access control, the network security policy, according to the respondents, was very ineffective at 8.7 percent, ineffective at 13.3 percent, moderately effective at 18.7 percent, effective at 43.3 percent and very effective at 16 percent.

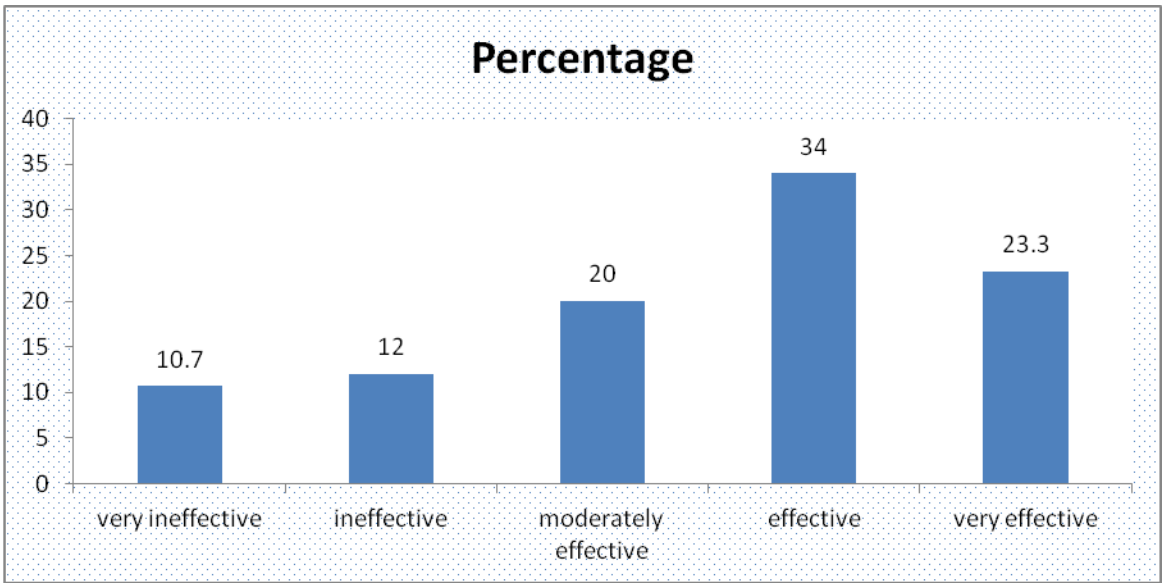


Figure 2 Levels to which Policy ensures risk mitigation, disaster recovery and business continuity

The security policy, according to figure 6 above, caters for risk mitigation, disaster recovery and business continuity at these levels; 10.7 percent- very ineffective, 12 percent – ineffective, 20 percent-moderately effective, 34 percent – effective and 32.3 percent – very effective.

Correlations and Regression Analyses

Relationship between On–job IT Security Training and Network Malware control

Malware is a technical name for malicious software in a network and its control of malware in the network is vital to ensure network security. It is expected that IT professionals who have on-job IT security training would attempt to put malware at bay, by taking a number of actions including; ensuring secure configurations for both hardware and software around all the hosts in their network. They should ensure that there is always anti-malware in the network, and that it is covered by the configuration assessment tools, including updates. Moreover, they should ensure that operating systems and other software used in the network are genuine, licensed and have necessary security updates as well as patches. It is therefore paramount for this study to explore the relationship between on job IT security training and the listed elements of Network malware control. The correlation results indicating this relationship summarized below.

Table2:Relationship between ICT Security Training and (malware control & policy implementation

Model elements	Pearson correlation	Sig.
Usage of anti- malware	.257**	.002
use of secure Network Operation systems	.385**	.000
Policy developed and internalized	.237**	.004
Policy conforms to industry standards	. 265**	.001
Policy enforces mandatory access control	.323**	.000
Policy ensures risk mitigation, DR and BC	.311**	.000
Policy controls behavior violation consequences	.335**	.000
Availability of critical servers and applications	.428**	.000
successful archive retrievals within 1 hour	.385**	.000

Table-2above reported a correlation coefficient values of (+ 0.257 and +0.237). This shows a weak positive relationship between on job IT security training the two elements of network malware control. Tables 23 and 24 (r = +0.302 and +0. 363 respectively) above show moderate positive relationship between the training and the respective elements of network malware control. An average correlation value thus gives (+0.257+0.302+0.363+ 0.237) /4 = +0.290. This means, that in general, there is a weak positive relationship between on job IT security training and then network malware control.

Relationship between On–job IT Security Training and Network Security Policy

Where network security is prioritized, operations, actions and reactions of techies are normally guided by a formal document – the network security policy document. This document establishes the rules that guide the behavior of users and IT personnel when handling network information systems and the consequences for violating the security policy. It gives guidance on data security, network access control / monitoring, as well as malware control. In some organizations, the document is contained within a general ICT policy document. Organizations therefore, develop the network security policy and internalize it to effectively control operations within the network infrastructure. The network security policy is only effective, if it is developed on the foundations of recognized industry standards, legislations and regulations. It should enforce

mandatory physical and logical access control to network resources by ensuring risk mitigation, disaster recovery and business continuity in case of disaster. The relationship between on job IT security training and the above elements associated with network security policy were investigated in this research, and responses were as tabulated below in tables / figures.

From the above results, there is positive relationship between on job IT security training and network security policy. The r values of (+0.237 and + 0.265) reported above indicate weak positive relationship between training and the two variables. However, reported r values of (+0.323, +0.311 and +0.335), pointing to a moderate positive relationship between on job IT security training and the corresponding sub-elements of network security policy. An average correlation value thus gives (+0.265+0.323+0.311+ 0.237+0.335) /4 = +0.294. Meaning that in general, there is a weak positive relationship between on job IT security training and then network security policy.

Regression model

$Qt = \beta_0 + \beta_3 MC + \beta_4 SP$ (Tobin's Equation)

Network Malware Control

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

Table 3: Regression analyses

Model elements	Un-standardized Coefficients		Standardized Coefficients	t	Sig.
	B	Standard error	Std. Error		
(Constant)	2.53	0.31		8.177	0.000
Malware control:	0.637	0.198	0.257	3.218	0.002
Security Policy	0.507	1.71	0.237	2.963	0.004

$$Qt = \beta_0 + \beta_3 MC + \beta_4 SP$$

For Network Malware Control and Network Security policy, the estimated model coefficients, the p – values ware less that 0.05 (i.e. $p = 0.002 < 0.05$ and $p = 0.004 < 0.05$) respectively, implying that Network Malware Control and Network Security policy are all statistically significant in predicting Tobin's Qt as well. Constant analyses' values for the two variables being (2.532 and 2.597) respectively, thus the final equation becomes in nd in average:

Qt = 2.56 + 0.532 MC + 0.507 SP

SUMMARY, CONCLUSION AND RECOMMENDATIONS

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.

SUMMARY, CONCLUSION AND RECOMMENDATIONS

Conclusions

The study found that ICT security training positively impacts on malware control as well as IT policy implementation in computer networks within Kenyan public Universities.

Recommendations

Hence, there is a need to seriously consider malware control as well as IT security policy implementation in computer networks in bettering information systems. It is recommended further that organizational heads should set aside budgets in support of ICT security training for ICT personnel to boost information systems' security management.

REFERENCES

Aguinis, H. & Kraiger, K., (2009). *Benefits of Training and Development for Individuals, Teams, Organizations and Society*. Annual Review of Psychology, vol. 60(4), pp. 51-74.

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

Baldwin, T., & Magjuka, R.J., (1988). *Transfer of training*: A review and directions for future research. Personnel Psychology review, vol. 41, pp. 63-105.

Barrett, A., & O'Connell, P. J., (2001). *Does training generally work*? : *The returns to in-company training*. Industrial and Labor Relations Review, 54(3) pp. 647-662.

Barry T. Hirsch and Terry G. (2012). Functional Form in Regression Models of Tobin's Q. Review of Economics and Statistics, The MIT Press, Vol. 75, No. 2. pp. 381-385.

Becker, H. S. (1960). *Notes on the concept of commitment*. The American Journal of Sociology, 66(1), pp. 32-40.

Birdi, K. S., (2005). *No idea? Evaluating the effectiveness of creativity training.* Journal of European Industrial Training, vol. 29(2), pp. 102-111.

Bishop. (2002). *Computer security: Art and science* , Addison-Wesley.

Cheswick & Bellovin., (2003). Firewalls and Internet Security, Second edition Addison-Wesley.

Clogg, C. C. (1979). Some latent structure models for the analysis of Likert-type data. Social Science Research, 8, 287-301

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

D'Arcy, Hovav, & Galletta., (2008). *User awareness of security countermeasures and its impact on information systems misuse information systems*. INFORMS Research Articles in Advance, pp. 1–20.

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

Heyes, J., & Stuart, M., (1996). *Does training matter*? *Employee experiences and attitudes.* Human Resource Management Journal, 6(3): 7-21.

Howard & LeBlanc., (2002). *Writing secure code,* second edition, Microsoft Press.

IBM Corporation., (2008). *Values of Information Security Training*. Retrieved from: [ftp://ftp.lotus.com/info/training/value-of-training_oct2008.pdf]

Mullard, S., (2007). *Network security: the impact of computer and network security in corporations today.* http://ttcshelbyville.files.wordpress.com/networksecurity.doc. *effectiveness.* Academy *of management review*, vol. 11, pp. 736-749.

Owens, P. L., (2006). *One more reason not to cut your training budget*: *The relationship between training and organizational outcomes*. Public Personnel Management, 35(2), pp.163-171.

Powanda, J., (1999). *Assembling a Curriculum for Various Security Disciplines*, 12th Annual FISSEA Conference, NIST.

Russell C., (2002). *Security awareness – Implementing an effective strategy.* [Available at http://www.sans.org/reading-room/whitepapers/awareness/security-awareness-implementing-effective-strategy-418]

Rubin., (2001). *White-hat security arsenal*, Addison-Wesley

Saltzer & Kaashoek (2009). *Principles of computer system design*, Morgan Kaufmann.

Steers, R. M., (1977). *Antecedents and outcomes of organizational commitment*. Administrative Science Quarterly, 22(1),pp. 46-56.

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