An assessment of Information Security Awareness among employees in Higher Education Sector in Zambia: A case of Zambia's public Universities.

Brian Halubanza
Mulungushi University
School of Science, Engineering and Technology
Kabwe, Zambia
bhalubanza@mu.ac.zm

Dr. Douglas Kunda
Mulungushi University
School of Science, Engineering and Technology
Kabwe, Zambia
dkunda@mu.ac.zm

Yolam Musonda
Mulungushi University, Kabwe, Zambia
yolammusonda@gmail.com

Abstract
The use of Information and Communication Technology to collect and process large volumes of data into information has made it possible for organisations to find ways and means of making informed decisions within a short space of time. There is so much dependent on information systems to such an extent that system failure can adversely compromise the organisation's operations. The education sector has not been left out but has instead become an information super house. The development of information systems has however not been spared by malicious activities, whether internal or external that tend to corrupt the much treasured information. (Alghananeem, Altaee and Jida, 2014)The way employees handle information flow in the organisation can either put the organisation at risk or can instead help protect the information and related information processing assets.

This study was therefore aimed at assessing Information Security Awareness (ISA) among employees in higher education sector in Zambia and how such levels contribute to information security efforts in higher learning institutions. The research was conducted by use of questionnaires grouped into five sections. The questionnaire was delivered to a total number of 150 employees from University of Zambia, Copperbelt University and Mulungushi University. The participants' years of service and level of education ranged from 1 year to over 10 years, and from Certificate to PhD holders respectively.

According to the findings of this research, it can be concluded that when employee self-awareness of information security, information security awareness training, Management's role in Information security awareness and information security awareness compliance monitoring improve, this is going to translate into improved Information Security (IS) in higher institutions of learning in Zambia as well. The results, in addition, also show that the higher learning institutions in Zambia do not attach the much needed support to information security awareness among its employees and there is also minimal support from top management.

***Keywords*—** Information Security; Information Security Awareness; Information Security Compliance; Cybercrime

Introduction
The adoption of information and Communication Technology (ICT) in the education sector demand that emphasis is put on the security of the critical information (Mani, Choo and Mubarak, 2014). It is believed that good information does not only enhance the competitive edge but also improves decision making in an organisation (Sharma and Dash, 2012). As part of their daily campus management, higher education institutions in Zambia do not only collect and process information but also share large volumes of data and as such there are a unique set of information security challenges that higher education institutions are facing. According to (CISSP, 2009), higher learning

institutions' Computer Systems are now being targeted for malicious activities especially that they are custodians of many records just like banks except that information from higher learning institutions is not difficult to access. There is, furthermore, a growing threat to information especially for learning institutions that are connected to a network (Mani, Choo and Mubarak, 2014).

A lot has been published about the need for higher education institutions in Zambia to embrace the Information and Communication Technology in their operations as well as in their curriculum (Isaacs, 2007). Much has also been published about the need for the higher education sector to adequately respond to society needs in enhancing the graduate's capacity to handle various ICT related challenges in the corporate world but what has not been clearly written about is how to respond to Information Security(IS) challenges that comes with the implementation of ICT in the higher learning institutions so as to safeguard the integrity of information while at the same time advocating for information security awareness among the employees as well as students (Cheung, 2014).

This research is hence focused on higher education sector in relation to information security awareness among employees in Zambia's public Universities.

Literature Review

Information and communication Technology has been globally acknowledged as being a growth contributor and a considerable driving force of many economies. Apart from reshaping the world's economies such as governments and societies, it's also being regarded as a source of job creation around the world (Bilbao-Osorio, Dutta and Lanvin, 2014). New industries as well as services are now emerging in various sectors of the economies across the globe. Among the sectors where ICT usage has increased include the education sector (World_Bank, 2010). ICT in the education sector in Zambia is seen as the basis for an increase in knowledge both in public and private sectors (Souter, 2010).

The education sector in Zambia has received a lot of support through the enactment of ICT policies that enhances the use of ICT and this has brought a lot of positive changes to the sector (Habeenzu, 2010). The ministry of higher education on the other hand oversees the operations of the learning institutions in Zambia and among its task is to see to it that information kept by the institutions of higher learning is only used for the intended purpose (Likando, 2010). Through its impact in social and economic sectors such as Education, Information and Communication Technology(ICT) usage contributes indirectly to Zambia's national development as well as the ability to achieve the Millennium Development Goals(MDGs) (Souter, 2010). According to (Isaacs, 2007), "*the recent adoption of a national ICT policy, as well as the development of a draft ICT policy for education and an associated implementation framework, provides an enabling policy environment to promote far greater access and use of ICTs across all sectors of Zambia's education system, including a system for enhancing education management, administration, and teaching and learning*". Furthermore, there is a growing trend in ICT integration in education and research development apart from that of other production sectors.

However, no efforts have been put in place to educate the masses in the education sector about the importance of information security as well as information security awareness especially among employees of higher learning institutions in Zambia. This has led to an increase in various crimes related to exploitation of ICT systems by employees in the education sector. According to the (CISSP, 2009), the major causes of data loss in the education sector is caused by improper data disposal, breach by insider, physical loss of hardware and electronic media and exploitation of system vulnerability as shown in figure 1-1.

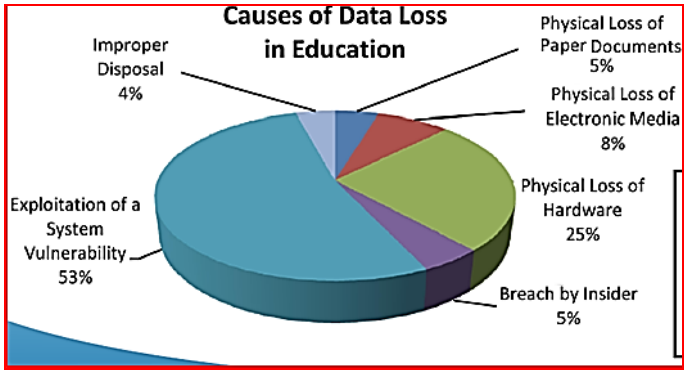

Figure 1: Causes of Data Loss in Education (Source: (CISSP, 2009))

Managing ICT systems with a view of protecting data without considering the human aspect in information security efforts may not yield the desired results because the major threats to information systems are the employees who come across various information by nature of their work (Chen and Li, 2014) (Blanke and Landry, n.d.). "The need for reliable and accurate information to achieve this, demands enhanced information security practices in these organisations. Sound information security practices require an effective information security program backed by information security awareness policies and frameworks"(Lukwesa and Upfold, 2011).

Information Security Awareness (ISA)

Information Security Awareness (ISA), defined as a state of consciousness and knowledge about security issues, is frequently found to impact security compliant behaviour (Haeussinger and Kranz, 2013). It is an organised and ongoing effort to guide the behaviour and culture of an organisation in regard to security issues (Tsohou et al., 2008). Information Security awareness, according to (Ahlan and Lubis, 2011) is "the extent to which organizational members understand the importance of information security, the level of security required by the organization and their individual security responsibilities and act accordingly". The usefulness of any Information Security measures cannot yield a positive outcome if the system users are not aware of the organisation's information security practices and policies (Siponen, Adam Mahmood and Pahnila, 2014). A good number of organisations are now becoming aware of the fact that in information security, employees are the weakest link and this recognition can enable organisations to also look at employees as the greatest asset in information security risk reduction (Bulgurcu, Cavusoglu and Benbasat, 2010). Similarly, "while the media headlines tend to focus on the spectacular events perpetrated by external hackers, employees inside an organization often pose silent but more dangerous threats than those outside the organization, due to their intimate knowledge about the organizational systems and the permissions they receive either properly or improperly for their work activities"(Hu et al., 2012).

Every individual is encouraged, in an organisation, to have basics and literacy in information security as it is a stepping stone between awareness and training as well as providing the foundation for information security terms and concepts (Kim, 2014). Similar to(Kruger, Drevin and Steyn, 2010), and because the aim of the research is to explore and assess the information security awareness of not only for information security professionals but all employee types, the generally used and commonly known concepts were used in the questionnaire. According to (Chan and Mubarak, 2012), the commonly used concepts include spam, phishing, social engineering, strong passwords and information integrity.

Information security awareness programs not only ensure that information is protected but also highlights the consequences of a security breach (Puhakainen and Siponen, 2010). The learning institution's reputation and assets can be put at stake and in serious jeopardy if employees' behaviour towards information security is not good (Siponen, Pahnila and Mahmood, 2010).

Understanding the attitude and ICT usage behaviour also plays a critical role in ensuring adherence to information security (Khan et al., 2011). (Ajzen, 2014) stipulates that there is, according to the Theory of Planned Behaviour(TPB), behavioral consistent prediction from information technology user's intentions. He further reiterates that changes in intentions have got an effect or rather results in behavioral change (Ajzen, 2014). Similarly, (Bulgurcu, Cavusoglu and Benbasat, 2010) also reiterates that "Since employees who comply with the information security rules and regulations of the organization are the key to strengthening information security, understanding compliance behavior is crucial for organizations that want to leverage their human capital". Studies have also shown that there is a positive effect on employee attitudes and improvements on compliance as a result of placing emphasis on information security awareness (Chan and Mubarak, 2012).

Managerial involvement

Information security awareness requires that top level managers be involved in implementing information security policies and practices for it to be effective. Similar to Hu (2012) and Chan & Mubarak (2012), there is a direct influence on management's involvement in information security awareness activities and employees compliance to information security policies. Organisations where leaders endorse security actions and behaviours achieve higher security awareness levels, and implementing a top down broad leadership style at division and unit levels helps to clearly spell out what organisation staff hear from executives and from their own managers(PricewaterhouseCoopers, 2013).

The organisation culture is also influenced by top management's participation and this ultimately impacts employees' attitudes and perceived behaviour control over compliance with information security awareness practices and policies (Hu et al., 2012). It was also echoed by Chan &Mubarak (2012) that "board level perceptions and thereby information security awareness are positively related to the strategic activities of an organization". Raising top management information security awareness can therefore ultimately improve the information security performance of the organisation (Susanto12, Almunawar and Tuan, 2012).

Information Security Awareness (ISA) Training

Information security awareness training plays a critical role in reducing the success of any hacking attacks at not only individual level but also the higher learning institution as a whole (Whitman and Mattord, 2013). Similar to (Kim, 2014) and (Maqousi, Balikhina and Mackay, 2013), a successful information security awareness program is one in which the focus is to ensure that an employee get a continuous secure behaviour. Similar to (Yayla, 2011) and (Siponen, Pahnila and Mahmood, 2010), training is one of the most common ways of ensuring that information security policies are adhered to by employees. The importance of training with regard to information security awareness levels cannot be overemphasized as it provides a good number of advantages such as the ease with which employees can increase and perfect their ability to interact with organisation software programs, and the skills gained are often regarded as determinants of not only intentions but also behaviour (Yayla, 2011) (Puhakainen and Siponen, 2010).

Information Security Awareness (ISA) compliance monitoring

Incentives in the form of rewards (Kirsch and Boss, 2007) and disincentives in form of sanctions (Willison, 2006) have been identified by various researchers as factors influencing the compliance of employees to security rules and regulations. The factors being referred to are normally individual based in the sense that they describe outcomes that have an influence on the employee as a result of either compliance or noncompliance to the information security policies of an organisation (Rauniar et al., 2014). According to (Bulgurcu, Cavusoglu and Benbasat, 2010), an employee's attitude is affected as a result of his or her personal belief concerning the consequences of complying or not.

In order to identify areas which need improvements, there is a need to assess employee information security awareness of the organisation as part of the overall organisational risk assessment strategies. In other words, the lack of information security awareness poses serious threats to an organization and must be properly risk assessed and mitigated (Kim, 2014).

The most extensive tool in Information security awareness assessment when assessing employees awareness levels, as proposed by (Chan and Mubarak, 2012) in ensuring a successful plan, should be in such a way that you start with developing a plan. According to a study carried out by (Chan and Mubarak, 2012) on university students, it was found that the use of the commonly used vocabulary test was of utmost importance and beneficial to gauging the information security awareness levels of employees. The above proposed vocabulary test was also used in this study where the focus was on employees rather than students.

The exploratory study conducted by Chinyama (2011) identified that in relation to information security management in Zambia, information security awareness activities as well as knowledge of cybercrime still remain a challenge (India, 2011). The study suggested that Zambian institutions do not have adequate security awareness programs in place to counteract the low levels of awareness, therefore compliance is also low. Thus it is important to adapt information security awareness programs that will not only foster a culture of compliance but will ultimately enhance staff compliance of information security (Conner and Sparks, 1996).

3.0 Research Methods

3.1 Research Approach

The quantitative approach was adopted when carrying out the research on assessment of information security awareness in higher education sector in Zambia.

3.4.1. Research Model

The proposed study's aim was answering the following research question; "How are the existing information security awareness efforts and practices among employees helping in ensuring the security of information in higher

education sector in Zambia?" The Model of this research was hence framed based on the literature review with a view of finding a proposed relationship between information security awareness and enhanced information security.

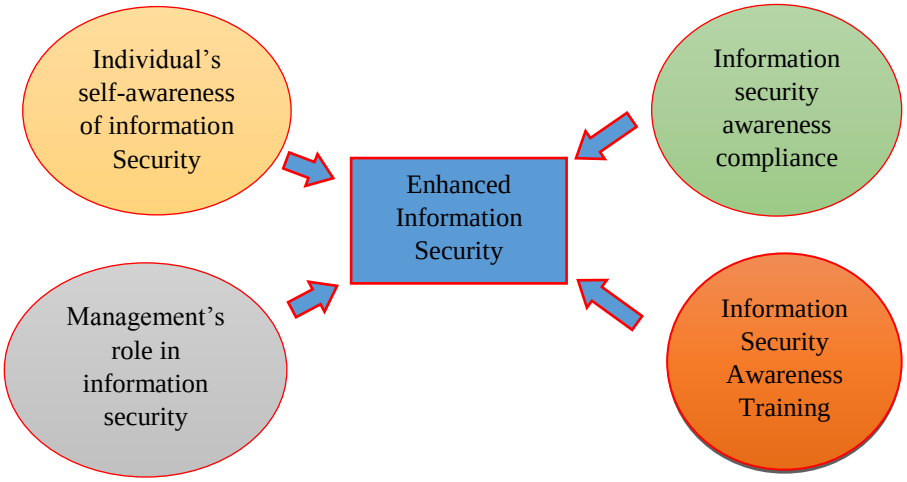

Figure 2: Research Model

3.2 Data Collection

The target population for this research were employees of higher learning institutions in Zambia namely; the University of Zambia, the Copperbelt University and Mulungushi University. The self-administered questionnaires that were used in this study consisted of pre-defined questions with predesigned response options that were answered in a specific order. An online questionnaire was also made available to cater for employees who are skilled with high levels of internet literacy who found it more convenience to respond to the questionnaires online (Saunders and Thornhill, 2009).

The sample size was calculated using Cochran (1997) formula as suggested by (Koskosas, et al., 2010) with prevalence estimated tolerance error which is 0.08 or 8% and confidence level equal to 1.96(Such that α =0.05). To cater for the non-response and blank cases, a total of 200 respondents where contacted within the chosen sector.

Findings

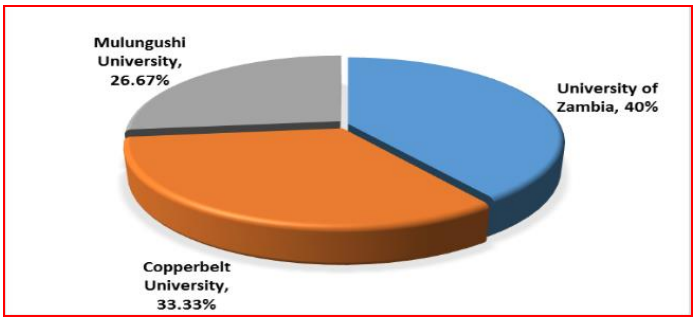

Figure 3: Questionnaire Distribution

	Frequency	**Percent (%)**
Female	63	42.0
Male	87	58.0
Total	**150**	**100.0**

Table 1: Gender Distribution

The total number of respondents drawn from Zambia's three public Universities in the survey were 150 out of which 58% (87 of 150) were males while 42% (63 of 150) were females.

In addition, the majority of respondents, 45.3% (68 of 150) were Master's Degree holders followed by 46 Bachelor's Degree holders making up 30.7% of the total respondents. 12.7% and 8.0 % of the respondents were Diploma and PhD holders respectively. 3.3% (5 of 150) of the respondents had certificates. Other descriptive statistics carried out included age of participants, respondent department, years of service and tasks performed at work.

Password sharing

			Level of Education					Total
			Certificate	**Diploma**	**Degree**	**Masters**	**PhD**	
Have you ever shared your work Password?	**Yes**	Count	3	13	14	27	3	60
		% within Level of Education	60.0%	59.1%	32.6%	39.7%	25.0%	40.0%
	No	Count	2	9	29	41	9	90
		% within Level of Education	40.0%	40.9%	67.4%	60.3%	75.0%	60.0%
Total		**Count**	**5**	**22**	**43**	**68**	**12**	**150**
			3.3%					
		% within Level of Education	**100.0%**	**100.0%**	**100.0%**	**100.0%**	**100.0%**	**100.0%**

Table 2: Password sharing

Based on the analysed data, there was a slight difference between the respondents who have shared their work passwords and those that have not. The results show that employees of the higher learning institutions in Zambia have not been spared from the practice of sharing passwords. This is shown from the results of the research in which 40% of the participants have shared passwords while 60% have not. The study revealed that 97.4% of those that feel that their computers are secure have in fact shared their passwords before. Furthermore, education levels also influence password sharing. Those with higher education levels tend to understand the importance of securing their passwords. Password sharing was more among lowly qualified employees such as Certificate (60%) and Diploma holders (59.1%). This indicates that more need to be done in the area of individual self-awareness of information security so as to overcome malicious practices such as password sharing practice which poses a risk to the confidentiality, reliability and integrity of information in higher learning institutions in Zambia.

Information security responsibility

	Departments		Employees		IT Staff	
	Frequency	Percent	Frequency	Percent	Frequency	Percent
Strongly Disagree	114	76.0	81	54.0	8	5.3
Disagree	10	6.7	44	29.3	20	13.3
Neutral	12	8.0	13	8.7	0	0.0
Agree	14	9.3	12	8.0	0	0.0
Strongly Agree	0	0.0	0.0	0.0	122	81.3
Total	**150**	**100.0**	**150**	**100**	**150**	**100**

Table 3: Information Security Responsibility

The results from a research questionnaire in which respondents were asked to state who they felt was responsible for information security in their respective institutions of learning revealed that 81.3 % of employees strongly agreed

that the Information Technology (IT) Staff are responsible for ensuring the security of information. How employees perceive information security responsibility has a significant effect on overall information security awareness efforts by the higher learning institutions. It's however, a responsibility of each employee regardless of the department to ensure that they adopt practices that enables the safety of information that comes their way by virtue of their work.

Knowledge of Website Policies

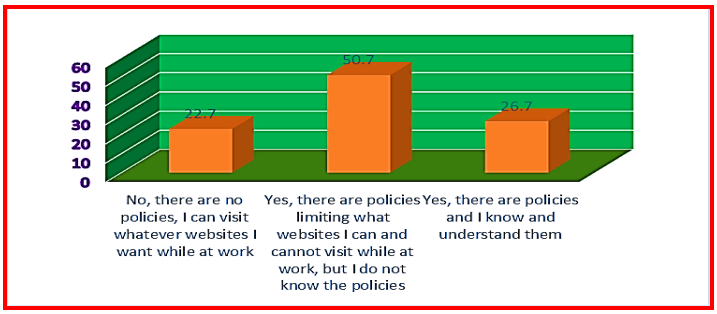

Figure 4: Website Policies

The findings show that 50.7% of total employees are fully aware or rather have an idea on the existence of website accessibility polices but are, unfortunately, not aware of the actual contents of the policies. This practice is not good since employees can still visit any website even the ones that could prove to be malicious to the institution's information thereby putting the organisation at an even higher risk.

Who to contact when hacked or if computer is infected

			University Department			Total
			Academic	Administration	IT	
Do you know who to contact in case you are hacked or if your computer is infected?	**Yes, I know who to contact**	Count	28	36	21	85
		% within University Department	51.9%	49.3%	91.3%	56.7%
	No, I do not know who to contact	Count	26	37	2	65
		% within University Department	48.1%	50.7%	8.7%	43.3%
Total		**Count**	**54**	**73**	**23**	**150**
		% within University Department	**100.0%**	**100.0%**	**100.0%**	**100.0%**

Table 4: Who to contact when hacked

The results from the research indicate that 43.3% of the total employees are not aware of who to contact when hacked or if the computer is infected. The implication of this is that this type of employees pose a risk to the institution's assets as well as the information.

Individual's self-awareness of IS and perception of improving information security in higher learning institutions in Zambia

		Perception of improving information security in higher learning institutions in Zambia
Individual's self-awareness of information security	Correlation Coefficient	.700**
	Sig. (2-tailed)	.000
	N	150
****. Correlation is significant at the 0.01 level (2-tailed).**		

Table 5: individual's Self-awareness of Information Security

A significant relationship exists between individual's self-awareness of information security and perception of improving information security in higher learning institutions in Zambia. The results therefore clearly indicate that if employees are aware of the basic facts and terms in relation to information security, there is a high chance that they will contribute positively to information security in an organisation or institution of higher learning. Employees who lack the basic knowledge about information security are more likely to fall victim hence increasing risk to the institution's information. This is evidenced by Spearman's strong Correlation Coefficient of 0.7. The findings are supported by (Mansky, 2008) who stated that there is a need by staff to demonstrate information security practices knowledge and that responses to security incidences can therefore be hampered or mishandled if employees are not aware of what a security compromise entails.

ISA training and perception of improving information security in higher learning institutions in Zambia

		Perception of improving information security in higher learning institutions in Zambia
Information security awareness training	Correlation Coefficient	.801**
	Sig. (2-tailed)	.000
	N	150
****. Correlation is significant at the 0.01 level (2-tailed).**		

Table 6: Information Security Awareness Training

The p-value of 0.01 indicates that there is a significant relationship between the two variables as indicated. The null hypothesis that there is no significant relationship between information security awareness training and perception of improving information security in higher learning institutions in Zambia is therefore rejected. Furthermore, the correlation coefficient of 0.8 also concludes that a strong relationship exists between information security awareness training and perception of improving information security in higher learning institutions in Zambia. Training of employees with regard to information security awareness not only equip them with the necessary knowledge but also helps to shape their behaviour and attitude towards information security (Veseli, 2011). The chi square test results shows that the p-value 0.000 hence rejecting the null hypothesis and adopting the alternative hypothesis.

The implication of not exposing employees to information security awareness trainings while expecting them to be self-aware of information security is that employees become a great threat to the security of information at the institution of higher learning.

Management's role in ISA and perception of improving information security in higher learning institutions in Zambia

		Perception of improving information security in higher learning institutions in Zambia
management's role in information security awareness	Correlation Coefficient	.803**
	Sig. (2-tailed)	.000
	N	150
****. Correlation is significant at the 0.01 level (2-tailed).**		

Table 7: Management's Role in Information Security Awareness

The results of the study clearly indicate that a significance relationship exists between management's role in information security awareness and perceived impact on information security awareness in higher learning institutions in Zambia. This conclusion is supported by results whose significant value (Sig. (2-tailed)) is less than 0.01. Consequently, the null hypothesis is rejected and the alternative hypothesis is accepted. A very strong correlation of 0.8 also exists between the two variables.

Pearson Chi-square p-value of 0.00 and the result that 0 cells (0.0%) have expected count less than 5 hence supporting the conclusion.

The role of management in information security awareness cannot be over emphasized. Management involvement not only sets precedence on information security practices but also motivates employees to adhere to laid down practices and procedures in relation to information security (Koskosas, Sariannidis and Asimopoulos, 2010).

Relationship between ISA compliance monitoring and perception of improving information security in higher learning institutions in Zambia"

		Perception of improving information security in higher learning institutions in Zambia
information security awareness compliance monitoring	Correlation Coefficient	.818**
	Sig. (2-tailed)	.000
	N	150
****. Correlation is significant at the 0.01 level (2-tailed).**		

Table 8: information security awareness compliance monitoring

The research findings show that a significant relationship exists between information security awareness compliance monitoring and perception of improving information security in higher learning institutions in Zambia. The p-value of 0.01 confirms the conclusion. The correlation coefficient of 0.8 and Chi square of 41 also indicate that a very strong relationship exists between the two variables. The null hypothesis is hence rejected. These results are in consistent with (Ong and Chong, 2014) and (Puhakainen and Siponen, 2010) findings.

Summary of findings

The findings showed that improved self-awareness of information security, Information security awareness training, management role in information security awareness and information security awareness compliance monitoring had an effect on the perception of improving information security in higher learning institutions in Zambia. It was also found out that more sensitization is needed to be done by both employees and management of the higher learning institutions in inculcating information security awareness practices. Having established that there was a significant relationship between the independent variables and the dependent variable, chi square analysis tests were also conducted to examine whether independent variables are actually dependent on the dependent variables. The results also showed that there was a significant relationship between the independent variables and the dependent variable.

Discussion of Results and Recommendations

Employees who are aware of information security terms and practices are not only a good asset to the organisation in relation to information security awareness but also help to instill confidence in the institution's efforts to secure information (Hadnagy, Aharoni and O'Gorman, 2010). The behaviour, knowledge and attitude of employees regarding information security awareness are an important aspect of information security awareness as highlighted in the literature review under the theories of behaviour.

Employees of higher learning institutions in Zambia do not have adequate training on information security awareness. The results from the research indicate that 74% of participants agree that there is basically no trainings offered at their places of work with regard to information security awareness. Information security awareness training is one of the typical or rather basic instruments that could improve or influence knowledge, behaviour and attitude among employees with regard to information security. Therefore, when employees attend information security awareness training, they become more information security aware. As such employees should receive more trainings in information security if institutions' efforts of ensuring the security of information is to yield fruits (Thompson, 2013).

As management pays particular attention to information security, there ivf 5frs a strong likelihood that employees will follow suit (Botha and Von Solms, 2004). Employees will look up to management practices and commitment in relation to information security awareness. As such, employees will be able to make decisions which could ultimately help improve information security awareness efforts of the institution.

Focusing on information security awareness monitoring among employees leads to efficiency and timely evaluation of information security awareness efforts and programmes leading to improvements in information security awareness. Managing information security awareness compliance monitoring helps to ensure that the information security practices and trainings are in line with the institution's information security strategies.

Recommendations

The need for Information security in the education sector has led many institutions of higher learning to embrace the various tools and practices that could help to secure information. Among such tools being harnessed by the higher institutions in Zambia include the development of Information Security Polices (ISP) which stipulates the institution's usage of information and protection of other physical computer network infrastructure. This cannot be achieved without involving employees. However, the study shows that most respondents were agreeable to the fact that not much is being done to inculcate good information security awareness practices among employees in higher learning institutions in Zambia.

The research not only focused on enlightening the higher education sector and stakeholders on the realities and challenges facing the higher education institutions in the area of information security awareness among its employees but also provide a framework that will assist them to gauge the effectiveness of their information security awareness efforts. The research findings will prove valuable in policy formulation with a special focus on information security awareness among employees in higher learning institutions and how such levels and practices could help in promoting information security. This will furthermore help higher education institutions to identify employees who could be change agents to a more security aware learning environment (Ong & Chong, 2014).

Results from this research not only contribute to Information security board of knowledge but will specifically seal any gaps in employee information security knowledge which if not traced could produce insecure behaviour at work. Gaps in Information Security Awareness (ISA), if any, could help the universities to invest in information security awareness initiatives. Creating awareness of the need to protect information, providing training in the skills needed to operate information systems securely, and offering education in security measures and practices is cardinal in information security.

Future Research

The use of qualitative methods in collecting data would add more value to the quantitative data from this research. Methods such as case studies and focus group discussions would be useful. Furthermore, inclusion of other education sector stakeholders in this research would add more value as well as provide answers to some of the missing information in this study. The research was based on anonymous survey hence making it difficult to even determine the level of information security awareness of each individual higher learning institution. Comparison of the information security awareness levels among institutions of higher learning is also recommended in future research.

References

Ahlan, A.R. and Lubis, M. (2011) 'Information security awareness in university: Maintaining learnability, performance and adaptability through roles of responsibility', Information Assurance and Security (IAS), 2011 7th International Conference on, 246-250.

Ahlan, A.R. and Lubis, M. (2011) 'Information security awareness in university: Maintaining learnability, performance and adaptability through roles of responsibility', Information Assurance and Security (IAS), 2011 7th International Conference on, 246-250.

Ajzen, I. (1991) 'The theory of planned behavior', Organizational behavior and human decision processes, vol. 50, no. 2, pp. 179-211.

Ajzen, I. (2014) 'The theory of planned behaviour is alive and well, and not ready to retire: a commentary on Sniehotta, Presseau, and AraÃºjo-Soares', Health Psychology Review, vol. 0, no. 0, pp. 1-7, Available: HYPERLINK "%20http://dx.doi.org/10.1080/17437199.2014.883474%20%0d%0a" http://dx.doi.org/10.1080/17437199.2014.883474 .

Alghananeem, K.M., Altaee, M.A. and Jida, B.K. (2014) 'The Impact of the Goals of Information Security Standards to Ensure Information Security', Journal of Management Research, vol. 6, no. 2, pp. 74-101.

Bilbao-Osorio, B., Dutta, S. and Lanvin, B. (2014) 'The global information technology report 2014: rewards and risks of big data', World Economic Forum, Geneva.

Blanke, S.J. and Landry, B.J. (n.d) 'Computer Abuse by Trusted Employees'.

Botha, J. and Von Solms, R. (2004) 'A cyclic approach to business continuity planning', Information management \& computer security, vol. 12, no. 4, pp. 328-337.

Bulgurcu, B., Cavusoglu, H. and Benbasat, I. (2010) 'Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness', MIS quarterly, vol. 34, no. 3, pp. 523-548.

Bulgurcu, B., Cavusoglu, H. and Benbasat, I. (2011) 'Information Security Policy Compliance: The Role of fairness, commitment, and cost beliefs'.

Chan, H. and Mubarak, S. (2012) 'Significance of Information Security Awareness in the Higher Education Sector.', International Journal of Computer Applications, vol. 60.

Chan, H. and Mubarak, S. (2012) 'Significance of Information Security Awareness in the Higher Education Sector.', International Journal of Computer Applications, vol. 60.

Chen, H. and Li, W. (2014) 'Understanding organization employees information security omission behavior: an integrated model of social norm and deterrence'.

Cheung, S.S. (2014) 'Information Security Management for Higher Education Institutions', in Pan, J.-S., Snasel, V., Corchado, E.S., Abraham, A. and Wang, S.-L. (ed.) Intelligent Data analysis and its Applications, Volume I, Springer International Publishing, Available: http://dx.doi.org/10.1007/978-3-319-07776-5_2.

Chinyama, S. (2011) 'The status of Cyber Crimes in Zambia', p. 66, Available: HYPERLINK "http://dspace.unza.zm:8080/xmlui/bitstream/handle/123456789/2096/sombochinyama00001.PDF?sequence=1" http://dspace.unza.zm:8080/xmlui/bitstream/handle/123456789/2096/sombochinyama00001.PDF?sequence=1 .

CISSP, D.B.T.W.J. (2009) 'FERPA and the Use of SSL Certificate Encryption to Protect the Security of Education Records', p. 7, Available: HYPERLINK "http://www.digicert.com/news/2009-10-13-digicert-education-white-paper.pdf" http://www.digicert.com/news/2009-10-13-digicert-education-white-paper.pdf .

Conner, M. and Sparks, P. (1996) The theory of planned behaviour and health behaviours., Open University Press.

Habeenzu, S. (2010) 'Zambia ICT Sector Performance Review 2009/2010', p. 42, Available: HYPERLINK "http://www.researchictafrica.net/publications/ICT_Sector_Performance_Reviews_2010" http://www.researchictafrica.net/publications/ICT_Sector_Performance_Reviews_2010 .

Hadnagy, C., Aharoni, M. and O'Gorman, J. (2010) 'Social Engineering Capture the Flag Results', Defcon 18 Social Engineering CTF.

Haeussinger, F. and Kranz, J. (2013) 'Information Security Awareness: Its Antecedents and Mediating Effects on Security Compliant Behavior'.

Howitt, D. (2010) Introduction to qualitative methods in psychology, Prentice Hall New Jersey NJ.

Hu, Q., Dinev, T., Hart, P. and Cooke, D. (2012) 'Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture*', Decision Sciences, vol. 43, no. 4, pp. 615-660.

Hu, Q., Xu, Z., Dinev, T. and Ling, H. (2011) 'Does deterrence work in reducing information security policy abuse by employees?', Communications of the ACM, vol. 54, no. 6, pp. 54-60.

India, R.B.o. (2011) 'Guidelines on Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds, Mumbai: Reserve Bank of India'.

Isaacs, S. (2007) 'ICT in Education in Zambia', SURVEY OF ICT AND EDUCATION IN AFRICA: Zambia Country Report, May, Available: HYPERLINK "http://www.infodev.org/infodev-files/resource/InfodevDocuments_436.pdf" http://www.infodev.org/infodev-files/resource/InfodevDocuments_436.pdf .

Isaacs, S. (2007) 'Survey of ICT and Education in Africa: Zambia Country Report'.

Khan, B., Alghathbar, K.S., Nabi, S.I. and Khan, M.K. (2011) 'Effectiveness of information security awareness methods based on psychological theories', African Journal of Business Management, vol. 5, no. 26, pp. 10862-10868.

Kim, E.B. (2014) 'Recommendations for information security awareness training for college students', Information Management \& Computer Security, vol. 22, no. 1, pp. 115-126.

King, E.M. (2010) 'Education and the Promise of the New Information Technologies', Seoul_Global_ICT_Forum_11-01-10, p. 30.

Kirsch, L. and Boss, S. (2007) 'The Last Line of Defense: Motivating Employees to Follow Corporate Security Guidelines', ICIS 2007 Proceedings, p. 103.

Koskosas, I., Sariannidis, N. and Asimopoulos, N. (2010) 'A survey in project commitment in the context of information security', Journal of Emerging Trends in Computing and Information Sciences, vol. 2, no. 2.

Kruger, H., Drevin, L. and Steyn, T. (2010) 'A vocabulary test to assess information security awareness', Information Management \& Computer Security, vol. 18, no. 5, pp. 316-327.

Likando, S. (2010) 'Universities and economic development: A case study of The University of Zambia (UNZA)'.

Lukwesa, C. and Upfold, C. (2011) 'Information Security Practices in Zambian Copper Mines: An Investigation Into the State-of-Practice of Information Security Within Zambian Copper Mines Based on the ISO/IEC 27002 Standard', Proceedings of the Second International Conference on Information Management and Evaluation, 281.

Mani, D., Choo, K.-K.R. and Mubarak, S. (2014) 'Information security in the South Australian real estate industry: A study of 40 real estate organisations', Information Management \& Computer Security, vol. 22, no. 1, pp. 24-41.

Mansky, B.R. (2008) 'Assessment of Information Security Awareness', June, p. 35, Available: HYPERLINK "http://www.winnipeg.ca/audit/pdfs/reports/ITSecurityAwareness.pdf" http://www.winnipeg.ca/audit/pdfs/reports/ITSecurityAwareness.pdf .

Maqousi, A., Balikhina, T. and Mackay, M. (2013) 'AN EFFECTIVE METHOD FOR INFORMATION SECURITY AWARENESS RAISING INITIATIVES.', International Journal of Computer Science \& Information Technology, vol. 5, no. 2.

Ong, L. and Chong, C. (2014) 'Information Security Awareness: An Application of Psychological Factors--A Study in Malaysia', 2014 International Conference on Computer, Communications and Information Technology (CCIT 2014).

Ong, L. and Chong, C. (2014) 'Information Security Awareness: An Application of Psychological Factors--A Study in Malaysia', 2014 International Conference on Computer, Communications and Information Technology (CCIT 2014).

PricewaterhouseCoopers (2013) 'Raising security awareness in your employees'.

Puhakainen, P. and Siponen, M. (2010) 'Improving employees' compliance through information systems security training: an action research study', Mis Quarterly, vol. 34, no. 4, pp. 757-778.

Rauniar, R., Rawski, G., Yang, J. and Johnson, B. (2014) 'Technology acceptance model (TAM) and social media usage: an empirical study on Facebook', Journal of Enterprise Information Management, vol. 27, no. 1, pp. 6-30.

Saunders, M.N.K.L.P. and Thornhill, A. (2009) 'Research Methods for Business Students'.

Sharma, D. and Dash, P.K. (2012) 'Effectiveness Of Iso 27001, As An Information Security Management System: An Analytical Study Of Financial Aspects', Far East Journal of Psychology and Business, vol. 9, no. 5, pp. 57-71.

Siponen, M., Adam Mahmood, M. and Pahnila, S. (2014) 'Employees' adherence to information security policies: An exploratory field study', Information \& Management, vol. 51, no. 2, pp. 217-224.

Siponen, M., Pahnila, S. and Mahmood, M.A. (2010) 'Compliance with Information Security Policies: An Empirical Investigation', Computer, vol. 43, no. 2, Feb, pp. 64-71, Available: ISSN: 0018-9162 DOI: 10.1109/MC.2010.35.

Souter, D. (2010) ICTs and development in Zambia: challenges and opportunities, London: Panos.

Susanto12, H., Almunawar, M.N. and Tuan, Y.C. (2012) 'Information security challenge and breaches: novelty approach on measuring ISO 27001 readiness level', International Journal of Engineering and Technology, vol. 2, no. 1.

Thompson, S.T. (2013) 'Helping the hacker? Library information, security, and social engineering', Information Technology and Libraries, vol. 25, no. 4, pp. 222-225.

Tsohou, A., Kokolakis, S., Karyda, M. and Kiountouzis, E. (2008) 'Investigating information security awareness: research and practice gaps', Information Security Journal: A Global Perspective, vol. 17, no. 5-6, pp. 207-227.

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

Whitman, M. and Mattord, H. (2013) Management of information security, Cengage Learning.

Willison, R. (2006) 'Understanding the perpetration of employee computer crime in the organisational context', Information and organization, vol. 16, no. 4, pp. 304-324.

World_Bank (2010) 'Global Symposium on ICT Use in Education: Building national ICT/education agencies', Available: HYPERLINK "http://web.worldbank.org/WBSITE/EXTERNAL/TOPICS/EXTEDUCATION/0,,contentMDK:22654587~menuPK:617610~pagePK:148956~piPK:216618~theSitePK:282386,00.html" http://web.worldbank.org/WBSITE/EXTERNAL/TOPICS/EXTEDUCATION/0,contentMDK:22654587~menuPK:617610~pagePK:148956~piPK:216618~theSitePK:282386,00.html .

Yayla, A. (2011) 'Controlling insider threats with information security policies'.