Asian Journal of Information Technology 17 (2): 142-152, 2018
ISSN: 1682-3915

An Assessment of Information Systems Security Management at University of Venda and its Impact to the University Community

Ratchel Chikurunhe, Armstrong Kadyamatimba and Willard Munyoka
Department of Business Information System, School of Management Sciences,
University of Venda, P. Bag X 5050, 0950 Thohoyandou, South Africa

Abstract: The study assessed the information systems security management at the University of Venda and its impact on the university community. It focused on identifying the critical information systems security measures that add value to the university and determines how the improvements in information security management can be achieved. The population pertaining to this research were academics and students. Qualitative and quantitative approaches were used in relation to data collection. Quantitative method was in the form of questionnaires and qualitative method was in the form of in-depth personal interviews. The study highlights improvement of security measures focusing on firewalls, antiviruses, policies, use of monitoring tools to detect intrusions and prevention of unauthorised information access. Factors of lack of qualified Information Systems Security (ISS) staff inadequate funding and absence or poor of ISS staff training programs must be looked at plus ISS awareness programs ISS policy reviews and constant software upgrades.

Key words: Authentication information systems, compliance, community information security management, highlights improvement, software upgrades

INTRODUCTION

The use of information has become a pervasive part of our daily life. People have become an information society (Xianping, 2009). Information is a critical resource for all organizations since, it supports business functionality and continuity. It helps managers and staff to make appropriate and effective decisions. Securing organizational information and its critical elements including the systems and hardware that use, store and transmit that information have become more and more important. Xianping (2009), also stated that information that has strategic value in organizations should be protected. Information is important asset as other important business assets for every organization (Erkan, 2006). It is crucial to an organization's business and must be protected properly.

Information security can be described as protection of information from various threats to ensure business continuity, minimize risks and maximize profits and business opportunities. Consequently organizations and governments become increasingly dependent on the availability, reliability and integrity of their information systems. Information security can be defined in terms of confidentiality integrity and availability (Puhakainen, 2006). Puhakainen also stated that information security plays an important role in protecting the data and assets of an organisation and there is news about security incidents such as defacement of websites, server hacking and data leakage. Organisations need to be fully aware of the need to devote more resources to the protection of information assets and information security should become a top concern in both government and business (Anonymous, 2008). Dhillon and Torkzadeh (2006) noted that the key to security lies not with technology but with the organization itself.

Literature review

Information and information systems: Information is one of the key resources for success of any organisation and managing it is equally important as managing other resources (Sarngadharan and Minimol, 2010). According to Hardcastle (2008), information maybe delineated as data that has been processed into an organised and usable form which is meaningful to the recipient for the task at hand. Hardcastle also defined systems as a collection of components that work together towards a common goal. A system has the main aim of

Corresponding Auhtor: Ratchel Chikurunhe, Department of Business Information System, School of Management Sciences, University of Venda, P. Bag X 5050, 0950 Thohoyandou, South Africa

receiving inputs and converting these into outputs. In systems, data which is the raw facts is used as the input for a process that makes information as the output.

Laudon and Laudon defined information system as a system either manual or automated that constitutes people, machines and/or systems organized to amass, process, transmit and distribute data that represent user information. Faud advocated that an information system is a set of interrelated components that collect (or retrieve), process, store and distribute information to support decision making and control in an organization. He further propounded that IS are designed to give managers the information they require as feedback. Furthermore, he suggested that the term information system is a generic reference to a computer based system that provides information processing capabilities for an individual or an entire organisation and provides the information enabling people to make better, more informed and prudent decisions. Whitman and Mattord (2010) emphasized that IS includes computer hardware, software, data, people and procedures.

Information systems security: According to Whitman and Mattord (2010), security is a state of being secure or to be free from danger. In other words, Whitman, defined information security as the protection of information and its critical elements. According to Qian (2010) ISS is defined as the protection of information and Information Systems from unauthorized access, use, disclosure, disruption, modification or destruction in order to provide integrity, confidentiality and availability. It further refers to access controls which deters unauthorized personnel from entering or accessing a system. Whitman and Mattord (2010) gave a different definition of information security. They defined it as the "protection of information and its critical characteristics (confidentiality, availability and integrity) including the systems and hardware that use, store and transmit that information, through the application of policy, training and awareness programs and technology. However, the most common element is of ensuring security measures to safeguard against unauthorised access. Therefore, information security is more of implementing security measures against an unauthorised access and this accession may be supported by Whitman and Mattord (2010) in their definition of information security. They referred to it as the "protection of information and the systems and hardware that use, store and transmit that information. If the organization cannot secure its information, severe impact on business continuity and business credibility can occur. If the organization's information assets are lost, passed into the wrong hands or in any wise are misused, it can be catastrophic to the organization. It will also be catastrophic to other parties doing business, directly or indirectly with this organization. It is of paramount importance that organisations understand the need to look after data contained in organisational systems. It is prudent to ensure that user training is undertaken without failure (Hardcastle, 2008). Having appropriate and effective information security control mechanisms in place to ensure the availability, confidentiality and integrity of information is both integral and critical to the process of security management (May and Lane, 2006).

Awad and Battah (2011) propounded that "information system security relates to the adequacy of management controls to guarantee the minimisation, prevention, detection and recovery from whole range of threats that could cause damage or disruption to computer systems. However, Pattinson (2008)'s view is contrary as he said that the process of information security cannot provide a complete prevention, avoidance, detection and recovery from the threats over it. Singh adopts both assertions but gives a solution to the conundrum. He argued that irrespective of the fact that IS management realizes that information security cannot provide complete prevention; the fact that any action of information security management can help to reduce these factors gives that motive to embrace all strategies, models and techniques to achieve that. Figure 1 provides for the main process of information system security based on Hussain et al's definition.

Information systems security management: According to Salahuddin (2011), the purpose of an organisation's information system is to provide access to its services anywhere at any time over closed and open networks and this leads to issues of security and privacy in the management of the information systems. Security pays its core traditional concerns to information properties of confidentiality integrity and availability. Salahuddin defined ISS management as ensuring business continuity and minimising business damage by preventing and minimising the impact of security incidents (Fig. 1).

Severe or enormous threats to any organisations IS in most cases are those that are caused by

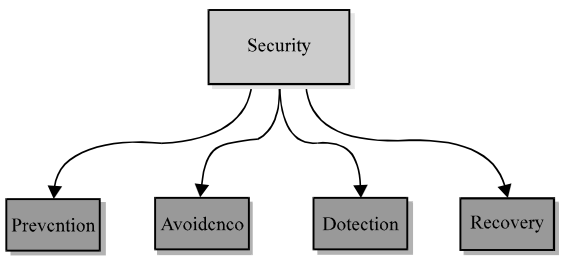

Fig. 1: Main process of IS security (Awad and Battah, 2011)

insiders. Insiders relates to employees and other stakeholders who have physical and/or logical access to organisational assets. Therefore, due to the severity of the risks posed to data by such insiders, it is essential that such risk is closely monitored and managed. The risk usually takes two forms, namely, risk that is posed by malevolent insiders who purposefully leak sensitive data for personal financial gain or other criminal purposes and the second risk is that of insiders who inadvertently create data exposures due to their imprecision or attempts to work around security measures. Dhillon *et al.* indicated that it is prudent that the behaviour of user's needs to be directed and monitored to warrant compliance with security requirements. It is of paramount importance to understand user behaviour characteristics because this helps to assess, improve and audit this behaviour, especially in the nature of security's dynamic changing environments. Recent literature documented that institutional cultures has influence on the implementation of information security management (Hsu *et al.*, 2012; Ransbotham and Mitra, 2009).

According to Stallings (2005), management face challenges in providing information security. Even for relatively small organizations information system assets are significant including databases and files related to personnel, company operation, financial matters and so on. About the above discussion, the management of information security should comprise of a framework for the university establishing policies and best practices. General awareness of security risk is essential to effective information security, Spears and Barki (2010) and D'Arcy *et al.* (2009) found that IS security policies, awareness programs and computer monitoring can lead to reduced intention to misuse Information systems. In agreement, policies, awareness programs and best practices contribute to effective management of ISS at the university.

Relevance of information systems security: The essentiality of ISS is that it provides for message integrity in addition to data confidentiality. Information, systems and hardware that support it are the lifeblood of any organisation which if compromised can have devastating consequences. According to Song, there are important costs which are related to ISS breaches. However in an information or knowledge based economy, assets are vested in people who informally network, hold and process information. Therefore, there should be steps to be taken, so that, the physical property will be protected and people in an organisation, similarly information security must be deployed to ensure that intellectual property is protected. Whitman and Mattord (2010) expostulated that the importance of information and its security is embodied in eight characteristics of information, namely: confidentiality integrity, availability, privacy, identification, authentication, authorization and accountability.

Security standards: Information security frameworks provides for the basic structures on which an organisation can 'hang' its security initiatives. Whitman and Mattord (2010) explained that these frameworks are divided into three main levels. The uppermost level consists of policies which are usually aligned with the organisation's mission and vision and updated as the organisation grows. They provide regulations for the protection of information assets within the organisation. At an intermediate level, standards are comprehensive statements of how the policies should be executed. At the lowest level, practices, guidelines and procedures facet how to comply with the policy or what must be done practically to comply with the organisation's information security policy as illustrated in Fig. 2. Organisations enable the adoption of any one of the several information security blueprints. These different frameworks focus on a variety of areas, mostly with documents aimed at the different levels, that is, policy, standards, guidelines or controls. Whitman and Mattord (2010), pointed out that security teams often knit together frameworks considered most applicable to an organisation's needs. Upon selection of the framework, a period of fine tuning will ensure that the framework best fit the organisations needs and vice versa. According to Norman and Yasin (2013), standards and best practices have been developed to assist in actualizing effective security in business. They further explained that while both standards and maturity measures can be used to improve IS security is S maturity can show the level of IS security as the framework shows the objective scale in categorising IS security.

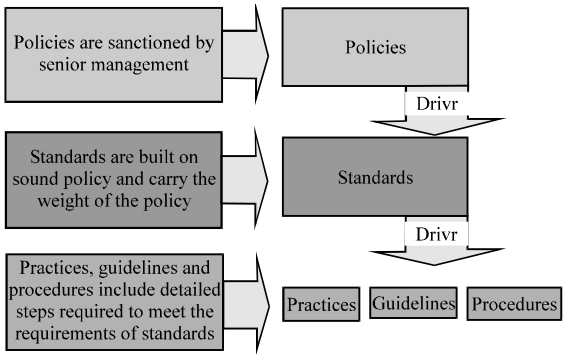

Fig. 2: Policies, standards, practices (Whitman and Mattord, 2010)

Problem statement: Information security in universities are considered more complex as compared to Information security used in commercial organizations even though it must pay the same attention to its stakeholders (Bose and Luo, 2011). As information security ensures a high quality of service which support and complement the business goals of the organization, the research focused on the importance of protecting information at the University of Venda. General awareness of security risk is essential to effective information security (Spears and Barki, 2010). Universities provide a source of the future leaders innovators and technical workforce through their core business of teaching, learning and research (May and Lane, 2006). This activity places university communities in a strong supportive and leadership role for the nation in general with respect to ensuring the security of information systems.

The University of Venda has had security incidents such as server hacking, denial of services and data leakages. Dealing effectively with threats to information involves the process of information security management to ensure that overall risks, costs and efforts are properly balanced within the university. Information include emails, examination results and biological details of students and staff which should be kept confidential. To avoid these security incidents, University of Venda senior management needed fully conscious of the need to put in place ISS to curb business risk associated with server hacking and data leakage.

Aim and objectives of the study: The aim of this study was to assess the information security management at the University of Venda and its impact on the university community. The objectives of the study were to:

- To determine the status of information security management in the university
- To determine the systems security problems encountered in the university
- Identify the critical ISS measures that add value to the university
- To determine how the improvements in information security management can be achieved

MATERIALS AND METHODS

The design of this research is divided into quantitative and qualitative methods to balance one another in terms of information from respondents and size of respondents (Tustin *et al*., 2010). According to Maree (2012), quantitative research has been defined as an objective measurement and statistical analysis of numeric data to understand and explain phenomena. It involves large samples examined through instruments that test a theory made prior to the study (Creswell, 2013). Quantitative research is accurate and more valid. On qualitative research, data will be generated frequently and it is difficult to quantify. On the other hand, qualitative research is a variety of research approaches that study phenomena in their natural settings without a predetermined hypothesis (Yin, 2011). Quantitative method was in the form of questionnaire which are issued to students and university staff to determine the security problems at the University and to determine the necessary improvements. Qualitative method was in the form of in-depth personal interviews with the IT department staff to provide more insight on the indicated research questions. Interviews aims to explore people's individual and collective understanding, reasoning processes and other significant factors in which may impact upon ISS management.

Population and sampling: The population pertaining to this research was the students studying Information systems, IT department staff and the university staff both academic and non-academic. The study employed purposive and convenience non-probability sampling. Due to the knowledge of the IT staff, purposive sampling was applied. The sample size for this research consisted of three groups namely, twenty academic and non-academic staff, thirty BIS students and four IT department staff.

Data collection: Quantitative method was in form of questionnaires and qualitative method was in form of in-depth interviews. Questionnaire survey was conducted to BIS students and the university staff. Personal in-depth interviews were carried out to IT department staff to acquire much detail from the systems users.

Data analysis and interpretation

Data was analysed to determine:

- The status of information security management in the university
- The systems security problems encountered in the university
- The critical ISS measures that add value to the University
- How the improvements in information security management can be achieved

Descriptive statistics was used on the questionnaire responses whilst thematic analysis was used on the in-depth personal interview responses. The statistical

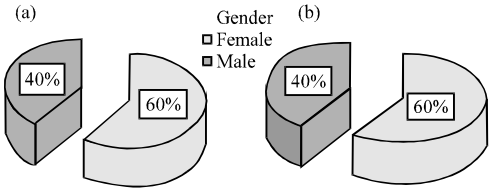

Fig. 3: Percentage of female and male participants; a) Staff and b) Students

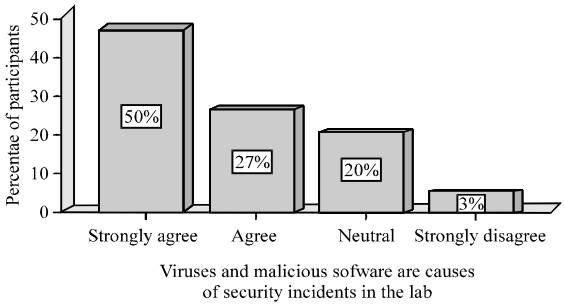

Fig. 4: Students views on viruses and malicious software

Package for Social Scientists (SPSS) and Microsoft Office Excel were used as tools for the analyses. The results are presented in frequency tables and graphs.

Demographic presentation: This consisted of the information concerning the population structure of the participants who participated in the study and is discussed in the subsequent sub-sections. This included the gender, age and marital status of the participants. The gender analysis shown on 1st pie chart of Fig. 3 indicated that the greater percentage of the staff members who participated were females made up 60% of the total respondents and forty percent of the respondents were males. The 2nd pie chart showed that 40% of the student participants were females and the greater percentage were males who made up 60%.

Causes of security incidents: In the following sub-sections, we briefly discussed the causes of security threats.

Viruses and malicious software: From Fig. 4, 50% of the students strongly agree and 27% agree that viruses and malicious software are causes of security incidents. About 20% of the students were neutral about this cause. A further three percent strongly disagreed to this notion. These might be a fraction of students who probably do not use the labs regularly.

Non-compliance: The part of the rationale of the study was to enlighten the University IT management on the

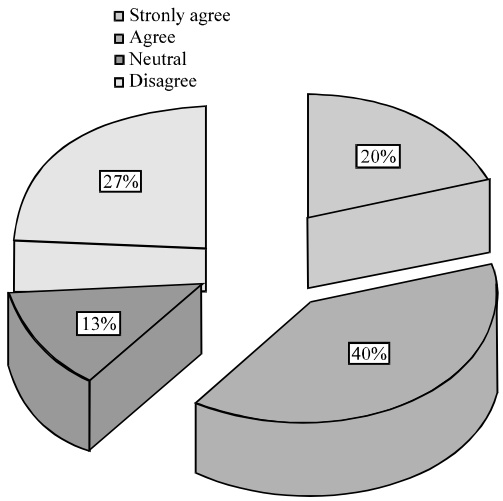

Fig. 5: Soft non-compliance (non-compliance to policies, guidelines and training programs is one of the major cause of security incidents)

causes of security incidents to allow proper management of ISS. On this question, the members of the staff's results are shown in Fig. 5. About 40% of the staff members strongly agreed and 20% agreed that non-compliance to policies, guidelines and training by both staff members and students cause security incidents at the university. A total of 27% of the staff did not agree with the notion. This might be because they assumed that every student or staff member at a tertiary institution is knowledgeable such that they would easily follow procedures and policies. However, for those who agreed, they have the perception that students and staff members should regularly be reminded to follow policies and procedures to avoid security incidents. One of the staff members had this to say in the in-depth interview: "our university have policies and procedure which are strong, if every person in the university can understand and follow such policies there will be low levels of security incidents at the university".

There is need for a strong call for students and staff members to read and understand these policies and thereby ultimately avoiding security incidents.

Measures of information security systems: In the following sub-sections, we briefly discussed the measures to security threats.

Clear direction in security procedures: On the question of whether clear direction in security procedures and roles is essential in improving security compliance to help in identifying the critical ISS measures which the university can employ to reduce security incidents both students

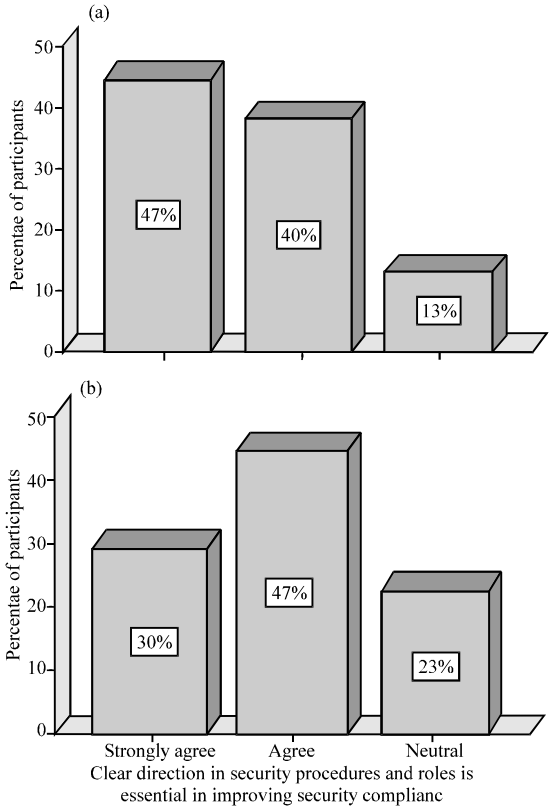

Fig. 6: Students and staff clear direction in security procedures. Clear direction in security procedures and roles is essential in improving security compliance

and staff members expressed that there is need for clear direction in security procedures for them to improve security compliance. Figure 6 showed us that 47% of students and 30% of staff members at the university strongly agreed that clear direction in security procedures should be imparted at University of Venda. The 40% of students and 47% of staff members agreed. Small percentages were neutral and this might again represent those participants who have no interest in the subject matter under discussion.

Training and education: For every implementation to be successful, care should be taken that proper training of the concerned parties is done. Students, lecturers and non-academic staff members should be given adequate and appropriate information security education and training. During the interview, on what the status of information security management practices is some of the respondents had this to say: "we are in the process of ensuring that when someone leaves a desktop in operation for three minutes it locks and server rooms are only allowed entry to a few authorized individuals".

Table 1: Training programs and securing computers cross-tabulation for staff

	Securing computers					
Variables	Strongly agree	Agree	Neutral	Disagree	Strongly disagree	Total
Training programs						
Strongly agree	1	2	1	2	1	7
Agree	0	1	0	2	0	3
Neutral	3	0	0	1	0	4
Disagree	0	0	0	0	1	1
Total	40	3	1	5	2	15

They also mentioned a lot of practices which should be in place and includes daily backups, use of firewalls which blocks irrelevant information flow and use of user passwords with a minimum of eight characters which makes it difficult for hackers to break such passwords. All these can be effectively achieved and fully utilized at the university if the students and staff are trained to secure their computers always, for instance, logging off their computers when moving from their work stations during tea or lunch breaks. On the rector scale from strongly agree to strongly disagree, the results in Table 1 were obtained pertaining to whether lack of training and awareness programs is one of the barriers towards achieving improved security compliance.

Table 1 shows that seven participants out of fifteen agree that staff have been trained to secure their computers always and three participants also agree that lack of training and awareness programs is one of the barriers towards achieving improved security compliance. This means that the university should set up workshops for training and awareness of staff members on the best ways to achieve improved security compliance. However, some programs already implemented has successfully dealt with the issue of securing staff computers in such a way that most staff members logoff their computers as they leave for tea break or lunch.

Computer literacy levels: It is also important to understand the computer literacy levels of students such that there will be proper evaluation of ISS management systems at the university. On the question that computer literacy levels can also compromise the information security systems at the institution, Fig. 7 shows that 30% of the students, strongly agreed and 47% agreed that computer literacy level compromise the information security systems at University of Venda, only three percent disagreed with this fact. These results implied that students were more willing to learn about new technologies and were also able to quickly understand any ISS measure which can be implemented at University of Venda. However, proper campaigns and awareness programs should complement effective implementation of any ISS measure for it to be successful.

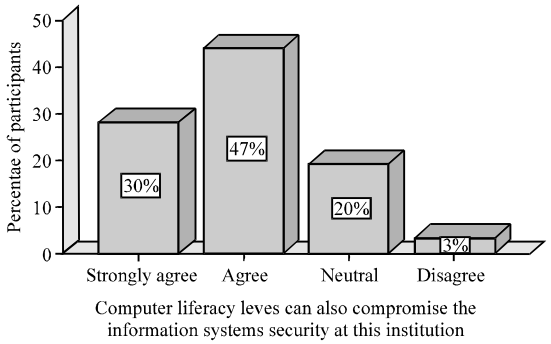

Fig. 7: Students views on computer literacy levels. Computer literacy levels can also compromise the information systems security at this institutions

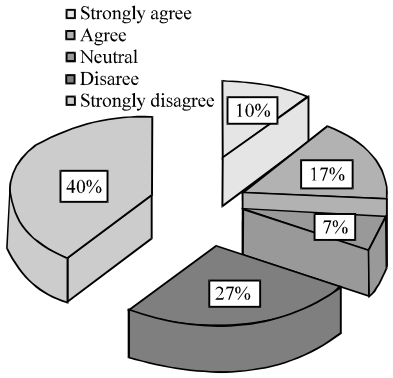

Fig. 8: Students views on changing passwards. In terms of logging into the computers in the lab, users can change their passwards at any time

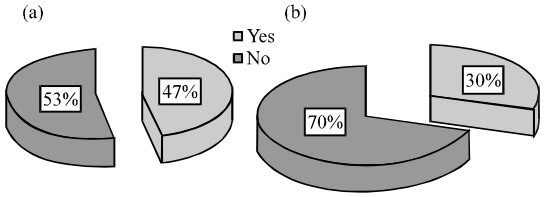

Fig. 9: Staff and students views on guidelines and regulations; a) Do you have rules and regulations concerning informations security issues at the institutions? b) Do you have guidelines concerning information security in the lab?

RESULTS AND DISCUSSION

Use of passwords and contingency plans: The answers to question on status of information security management practices brought up answers which discussed usage of long passwords by users and some contingency plans such as backup, antiviruses, authentication and firewalls. Some of the respondents in the interview were noted saying: "the university is making use of monitoring tools to detect intrusion such as access controls, firewalls. There is also use of eight-digit passwords, daily backups and antiviruses in place".

Responses from the interview also confirmed that, the university has measures for ensuring ISS in place such as authenticating users when logging on to the system. However, these measures require improvement, so that, the university will be well positioned to effectively detect and defend against security incidents including cyber-attacks and malicious software. Figure 8 revealed information pertaining to the ability to changing their passwords at any time.

About 40% of the students chose to remain neutral and 27% disagreed to the question. The reason for this might be attributed to the fact that they bring their own laptops in the labs which makes them reluctant to changing their desktop password regularly. Only 27% agreed to the question. These might be students who use the computer labs regularly and were fully aware of the importance of securing information.

Management of security incidents at the university: In the following sub-sections, we briefly discussed how ISS can be managed.

Guidelines and regulations: The other purpose of the study was to determine how the improvements in information security management can be achieved. The general question for the students and staff in this survey was whether proper guidelines or regulations concerning ISS are in place at the university.

From the 2nd pie chart on Fig. 9, 70% of the students agreed that they have guidelines concerning ISS in the lab and 50% of the staff members on the 1st pie chart agreed that there are rules and regulations concerning information security issues at University of Venda. Therefore, the only concern for IT management employees will be to have awareness campaigns which will make sure that such guidelines, regulations, policies and procedures are well understood by students and staff members at the university.

Antiviruses and backup: The data collected from the questionnaire on the question on whether or not there are antivirus to detect and defend against cyber-attacks and malicious software showed that 70% of students do not have antiviruses while 73% of the staff member have antiviruses on their computers (Fig. 10). A greater challenge to the management will be to ensure that there

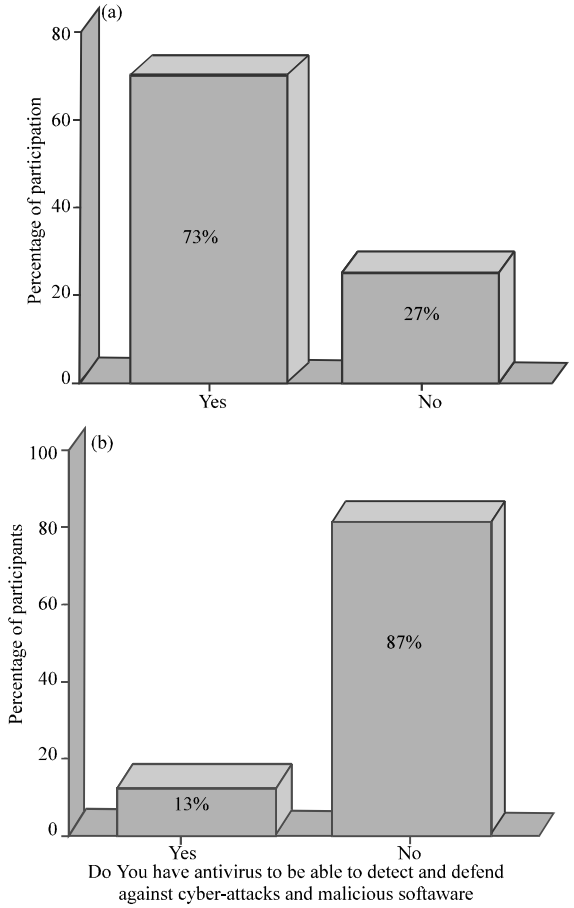

Fig. 10: Staff and students use of antiviruses; a) Staff and b) Students

Table 2: Staff backup views

	Percentage		
Variables	Frequency	Valid	Cumulative
Yes	14 (93.3)	93.3	93.3
No	1 (6.7)	6.7	100.0
Total	15 (100.0)	100.0	

are installations of antiviruses software in all the student labs. On contrary, a manageable number of staff at the university should be made aware of the use of antiviruses. However, greater efforts are being done as confirmed from the interview to ensure secure computers to students to avoid potential security breaches.

Table 2 shows findings from staff members on backup which indicated that fourteen of the fifteen participants from the staff confirm that there are aware that they should constantly backup their information to prevent information loss.

Problems and suggestions: In the following sub-sections, we briefly discussed the problems and the suggestions.

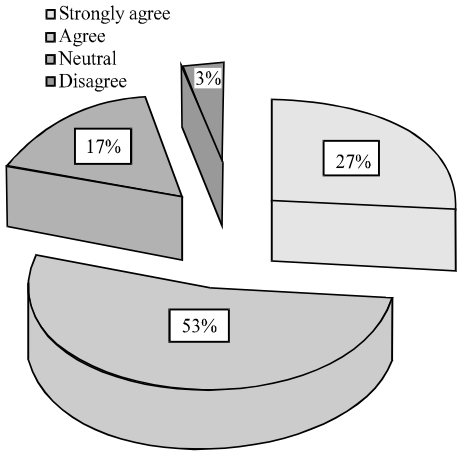

Fig. 11: Students views on technology. Inadequate technology can be considered a barrier to achieving improved security compliance

Major problems at the university: On trying to look on what should be done to improve ISS on the university, it is important to single out the major problem which was obtained from the survey. Students and lecturers confirmed lack of adequate technology at this institution as a barrier to achieving improved security compliance. Figure 11 depicts that 80% of the students regard inadequate technology as a barrier in achieving improved security compliance. Management and staff at the IT department are clearly aware of this as a problem hence efforts are done to secure funds which will help in improving technological infrastructure at University of Venda.

Impacts and suggestions for improvement: The last two questions of the two questionnaires probed on the impacts on issues such as maintenance of privacy integrity issues, concerns on hackers and fear of unauthorized access. Furthermore, security measures such as use of finger prints to enter the labs, tight fastening of cables increased training and awareness programs, regular updates and lab polices and installation of antiviruses in student's labs were suggested by the staff and students. Figure 12 shows how staff members are affected by ISS. Most of the staff members at University of Venda revealed how the ISS affects them; privacy concerns, lessened confidence due to poor security. They feel the university should put in place measures to maintain confidentiality and integrity issues to improve the fear of data loss and unauthorized access on computers among individuals.

Suggestions from staff and students: Some suggestions to do away with such responses are depicted in Fig. 13.

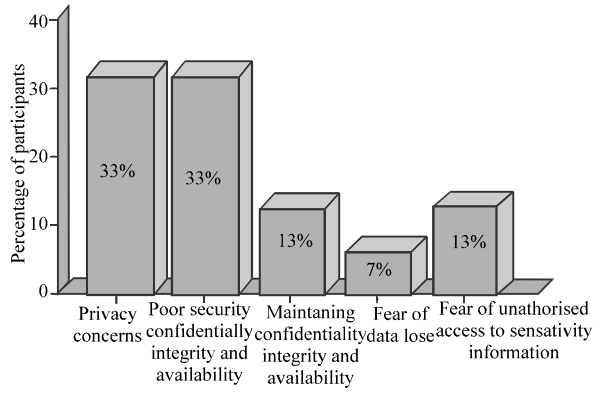

Fig. 12: Impacts on staff members. How does information systems security affect you as a staff members?

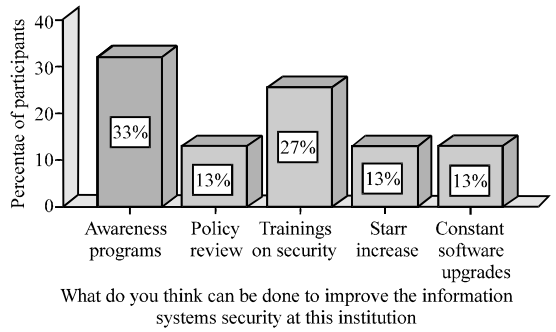

Fig. 13: Suggestions from staff members

Table 3: Student's suggestions

Variables	Percentage		
	Frequency	Valid	Cumulative
Updates needed	4 (13.3)	13.3	13.3
Use of fingerprints to enter the lab	7 (23.3)	23.3	36.7
Lab polices	3 (10.0)	10.0	46.7
There should be training programs	3 (10.0)	10.0	56.7
Tight fastening of cables	4 (13.3)	13.3	70.0
Good password management	2 (6.7)	6.7	76.7
Authorized students should enter the lab	3 (10.0)	10.0	86.7
Installation of antiviruses in labs	4 (13.3)	13.3	100.0
Total	30 (100.0)	100.0	100.0

staff members suggested awareness programs, policy reviews, training on security, more IT staff and constant software upgrades as measures to end the problems mentioned in earlier discussion on how ISS affect them. Students mentioned many suggestions which are depicted in Table 3. BIS students strongly recommended that gaining access to the lab should be through biometrics, tightly fastening of cables and regular software updates which include installation of antiviruses in the labs. Student's suggestions, especially, the use of biometrics to gain access to the lab requires a large amount of capital and more qualified staff at the institution.

ISS has been clearly described in the study as the protection of information and IS from unauthorized access, use, disclosure, disruption, modification or destruction to provide integrity, confidentiality and availability. The IT department at University of Venda is faced with a task of protecting the institution's information and influence staff and students to follow guidelines and procedures to keep their information safe. They should use the embodied in eight characteristics of ISS namely, confidentiality integrity, availability, privacy, identification, authentication, authorization and accountability to come up with security standards to enable effective ISS management. One of the objectives of the study was to identify the critical ISS measures that add value to the university.

It can be seen from the survey that, if the management can strategically adopt effective ISS management practices, it will be possible that all information problems together with security incidents at the institution will become a talk of the past.

The study supported that ISS is important and has positive impact on the university community. The study revealed the status of ISS management practices at the university and the improvements to ISS that can be implemented by the senior management. These include the use of firewalls and antiviruses, policies, backups, use of monitoring tools to detect intrusions and access of information to the authorised individuals. The study revealed problems being faced at the institution and most respondents suggested that there should be an increase in IT staff members who will specialize on the security of the information systems, regular awareness programs, policy reviews. The research also clarified the major security standards which provides for the basic structures on which an organisation can 'hang' its security initiatives and answers the research questions.

CONCLUSION

It can be concluded that it is important to convince IT managers about the benefits of IS security decisions and to raise their awareness towards types of IS security measures to raise management involvement in IS security decisions. It is imperative for IT managers to make careful considerations on the cost benefit analysis before implementing ISS strategies. Problem which managers are facing concerns vandalism from students inadequate technological infrastructure and those students who do not want to learn and follow procedures. Such students and staff must be persuaded and educated in such a way that they understand all the benefits of ISS practices in keeping information safe. While challenges are faced in providing adequate infrastructure, IT managers at

universities should also understand that there are potentials for extraordinary returns on investment in keeping information safe. From the study, we can safely conclude that strong security management skills are a prerequisite for successful ISS management. These skills are also important in strategy formulation and long-term alignment of ISS goals to the general objectives of the University

RECOMMENDATIONS

The study also came up with critical contributions and issues which can be used by the University to reduce security incidents which among others at the University are: creating new security measures were students can be allowed access to labs using biometrics, allowing the authorised group of students to get access to their labs. An increase in personnel in the IT department which will allow for effective implementations of proposed Information security management principals. Installation of antiviruses in the student's computers in laboratories, laptops and staff's computers will effectively deal with malicious software attacks. It is recommended that managers should understand early years of ISS were a technological success with the digital infrastructure created to sustain growth of internet usage. This will help managers in conceptualizing all the important aspects underlying ISS management. The management should consider making use of a security monitoring system. Security monitoring will provide a way of confirming that information resource security controls are in place, effective and are not being bypassed. The IT management can also consider disabling network access to any device that is not protected sufficiently or infected with a virus. The devices will gain the network access after the device has been cleaned, application patches, antivirus software and applicable operating system have been installed. In terms of access control, the IT management should make sure that the student bar codes are changed every year to ensure that access to the labs is only to the registered students. Training and awareness programs should be carried out regularly to the university community, so that, they will be fully informed about the importance of ISS.

REFERENCES

Anonymous, 2008. An overview of information security standard. The Government of the Hong Kong Special Administrative Region, Hong Kong.

Awad, H.A. and F.M. Battah, 2011. Enhancing information systems security in educational organizations in KSA through proposing security model. Intl. J. Comput. Sci. Issues, 8: 354-358.

Bose, R. and X. Luo, 2011. Integrative framework for assessing firms' potential to undertake Green IT initiatives via virtualization: A theoretical perspective. J. Strategic Inf. Syst., 20: 38-54.

Creswell, J.W., 2013. Research Design: Qualitative, Quantitative and Mixed Methods Approaches. 4th Edn., Sage Publication, Thousand Oaks, California, USA. ISBN:978-1-4522-2610-1, Pages: 265.

D'Arcy, J., A. Hovav and D. Galletta, 2009. User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. Inf. Syst. Res., 20: 79-98.

Dhillon, G. and G. Torkzadeh, 2006. Value-focused assessment of information system security in organizations. Inf. Syst. J., 16: 293-314.

Erkan, A., 2006. An automated tool for information security management system. Master Thesis, Department of information systems, Middle East Technical University, Ankara, Turkey.

Hardcastle, E., 2008. Business Information Systems. Elizabeth Hardcastle & Ventus Publishing, USA., ISBN:978-87-7681-463-2, Pages: 54.

Hsu, C., J.N. Lee and D.W. Straub, 2012. Institutional influences on information systems security innovations. Inf. Syst. Res., 23: 918-939.

Maree, K., 2012. Complete Your Thesis or Dissertation Successfully: Practical Guidelines. Juta Publisher, Cape Town, South Africa, ISBN:9780702189166, Pages: 262.

May, L. and T. Lane, 2006. A model for improving e-security in Australian universities. J. Theor. Applied Electron. Commerce Res., 1: 90-96.

Norman, A.A. and N.M. Yasin, 2013. ISS Management (ISSM) maturity factors in E-commerce Malaysia. Aust. J. Basic Appl. Sci., 7: 165-173.

Puhakainen, P., 2006. A design theory for information security awareness. Master Thesis, Faculty of science, Oulu University, Oulun Yliopisto, Finland.

Qian, Y., 2010. Mitigating Information security risks during the transition to integrated operations: Models and data. Ph.D Thesis, University of Bergen, Bergen, Norway.

Ransbotham, S. and S. Mitra, 2009. Choice and chance: A conceptual model of paths to information security compromise. Inf. Syst. Res., 20: 121-139.

Sarngadharan, M. and M.C. Minimol, 2010. Management Information System. Global Publisher, Mumbai, India,.

Spears, J.L. and H. Barki, 2010. User participation in ISS risk management. MIS. Q., 34: 503-522.

Stallings, W., 2005. Cryptography and Network Security Principles and Practices. 4th Edn., Prentice Hall, USA.

Tustin, D.H., A.A. Ligthelm, J.H. Martins and H.D.J.V. Wyk, 2010. Marketing Research: In Practice. 1st Edn., Business Print, Pretoria, South Africa,.

Whitman, M. and H. Mattord, 2010. Management of Information Security. 3rd Edn., Cengage Learning, Boston, USA., ISBN-13:978-1-4354-8884-7, Pages: 520.

Xianping, W., 2009. Security architecture for sensitive information systems. Ph.D Thesis, Faculty of Information Technology, Monash University, Melbourne, Victoria.

Yin, R.K., 2011. Qualitative Research from Start to Finish. Guilford Press, New York, USA., ISBN:978-1-60623-701-4, Pages: 348.