Proc. of the Second Intl. Conf. on Advances in Computing, Electronics and Electrical Technology - CEET 2014.

ISBN: 978-1-63248-034-7 doi: 10.15224/ 978-1-63248-034-7-29

Information Security Awareness and Practices In Malaysian IHLs: A Study at UNISEL

[Ishak, I.S., Ishak, I.S., Abu Hassan, R., Suradi, Z., Mansor, Z.]

***Abstract*- Securing information is essential for safeguarding an organization business operation since information is a valuable asset for the organization. One of the most vital information security controls is information security awareness and practice. The purpose of this study is to assess the levels of information security awareness and practice among faculty staffs in Malaysian IHLs. The survey questionnaire was distributed to faculty staffs in University Selangor as a sample study to assess the trend of information security awareness and practice. The finding of the study shows that more than half of them were aware of the importance of information security in educational learning environment. This research is expected to contribute to information security awareness in IHLs. This research recommends that an information security policy should be developed for Malaysian IHLs.**

Keywords—*information security, information security awareness, security, information security policy, risk assessment*

I. Introduction

Information security is one of the important issues discussed in Institutes of Higher Learning (IHLs). It is because securing information is essential for safeguarding the organization business operations and reducing the risk of information theft [1][2][3]. Several studies show that IHLs had experienced several attacks on their information resources. The examples of information security attack are information security breach, virus used to broadcast confidential information; hacker gain access to faculty members names and social security numbers [4][5][6]. This situation shows that IHL's is open to attack from a hacker, and the organizational information is at risk. The IHLs need to evaluate the organization information security risk continuously. Similarly, Smith and Frisby pointed that risk assessment is the first step in creating an information security policy[7]. Hence, the objective of this study is to investigate the level of information security–awareness and practices among faculty staffs in Malaysian IHLs. Faculty of Computer Science and Information Technology, Universiti Selangor (FCSIT, UNISEL) was chosen as a case study as the Malaysian IHLs context is quite similar from one to another. The study is interested to identify the faculty staff computing behaviors that would affect the vulnerability of IHLs information security attacks and assess the occurrence of unsafe computing behaviors.

Izwan Suhadak Ishak, Irny Suzila Ishak, Rohaya Abu Hassan, Zulkefli Mansor
Universiti Selangor
Malaysia

Zurinah Suradi
Universiti Kuala Lumpur
Malaysia

This study will enable FCSIT and Centre of ICT at UNISEL to evaluate their information security training programs and their computer and information security policies. This research is important to create awareness and propose action to ensure the staff can protect their information resources and protect their people from any information security attacks. This article describes information security issues and describes information security in Malaysia IHLs. It discusses the methodology and finding of the study. This research shows that IHLs should take proactive steps to encounter this information security attack and challenges.

II. Literature Review

A. *Information Security Issues*

Information security has long been the concern of organizations. This awareness encourages organization to find ways on how to protect the information. One of the efforts is by inventing encryption code and integrating the encryption code with computer technology [1][8][9][10]. Information Security is defined as all action taken to protect and preserve the confidentiality, integrity, authenticity, availability, and reliability of the information. This indicates that information systems may be secured by preventing, detecting, and correcting internal and external threats [2][3][11].

Nowadays most industries are dependent to information technology (IT) to store their organizational information. In order to ensure the system can sustain, all security aspects must be addressed carefully. This action is to avoid any security breach or incidents. In addition, end user must be equipped with at least the basic information security knowledge that enable them to detect threats and in turn may prevent the threats from occurring. However, with the rapid evolvement of ICT, information security breaches scenarios are increasing [12][13][14][15]. In the early days, the viruses attack did not cause any serious damage to the computer system. Currently, as there are many types of computer security attack occurred, it may affect critical information and in turn will damage the continuity of organizational functionality and business process. Today, with the cloud technology advancement, ICT has allowed information to be shared unexceptionally, making that information more susceptible to attack. For instance, computer networks like the Internet provide convenient access to information as well as a convenient point of attack for service disruption and information theft [16]. Hence, this makes many organizations to be more prudent especially when using the online system in conducting online activities or transactions.

Proc. of the Second Intl. Conf. on Advances in Computing, Electronics and Electrical Technology - CEET 2014.

ISBN: 978-1-63248-034-7 doi: 10.15224/ 978-1-63248-034-7-29

Although developers and researchers have provided ways to secure their computer networks, some authorized users still can unconsciously engage in practices that expose the host systems to attack. Bishop stated that "the heart of any security system is people"[17]. This implies that users who are uninformed about information security and indifferent to information security problems tend to act in ways that may increase the risk of security breaches and attacks. Meanwhile, users who are aware of these problems can implement protective measures that help to reduce the risk of information security attack.

Previous research had discussed several issues regarding information security that include the following: information security challenges, technical computer security issues, and information security awareness. According to Thomson and Solms, a great challenge has been brought by the availability of the personal computer, increasing use of internet and the development of the system that do not consider security measures[18]. It shows that the emergence and development of technology had affect information security. Each technology has its pros and cons. For example, Internet usage can bring the user to borderless information searching which at the same also bring borderless virus attack. Further, Internet and computer user is not limited to workers at an organization but, also included home users as well. As a result, the attack targets become broader when home users can also become a victim.

Furthermore, attackers have matured in using their hacking skills where they can avoid the authentication process to access each other's files as in the theft of confidential information [10]. Currently, most of our information resides on the electronic database and attract the adversary for social engineering, phishing, identity theft and another white collar crime. In addition, if users are not aware with the new type of stealing, they can easily expose their sensitive information and become a victim of the attack.

Besides the technical computer security issue, information security awareness issue must be looked into as well. Today's security problems are primarily due to the lacking security awareness of users. However, it can be encounter without the need of sophisticated security technologies [11]. This indicates that the human factor is an important factor. However, there is a need to avoid human error factor. For this reason, it is important to create awareness among the user.

The term "information security awareness"' is used to refer to a state where users in an organization are aware of the ideally commitment to their security mission (often expressed in end-user security guidelines) [19]. User must understand and be knowledgeable regarding IT security threats in order to ensure that they can react properly to any security incidents. This is because although the best security technology has been implemented, it has been shown that it cannot avoid other types of security attack to occur because of human error factor.

A survey on the security perception of personal novice Internet user at United Kingdom (UK) shows that 43% of the respondents claimed that they do not understand the threats, 38% asserted they did not know how to use security packages, 35% indicated that they did not know how to secure their computer, and 32% stated that they did not know about the threats [20]. Besides that, the study also reveals that 17% of the respondents had systems that were used by children under 12, whereas 18% them had computers that were used by their children aged 12–18 (the overall proportion of respondents with children was 30%).

With the advent of Internet users, the focus of information security awareness has become broader where it does not only cover end user at organization; it also requires others who use Internet at home to be aware as well. Further, Furnell also found that the fact that organizations are tightening their defenses leaves home user systems as attractive targets for compromise [20]. As for the security aspects, whether, in terms of physical or logical, which are not being focused by home user, it leaves vulnerable for them.

B. Information Security in IHLs

Institution of Higher Learning (IHL), is an entity that is responsible for preparing a knowledgeable and high-level manpower for the country. The institutions needs to take full advantage of the rapid growth of technology by embedding and implementing the Information and Communication Technology (ICT) into their day to day operations; either in business operations or academic practices. However, with the rapid and fast emerging of technology, the information security aspects pose major challenges to the institutions in guarding their confidential information since IHL's database are open to risk and attack.

Institutes of Higher Learning (IHLs) are at special risk for information theft. The reasons why university is under attack are because university are easy targets, and they store information assets such as employee data, patient health information, scientific research data and information from classified government programs. University is an easy target because it has an open structure, have long retention periods, facing significant budget constraint which limits technology and security investment [21]. For examples, more than 309,000 data of the University of Maryland student, staff and alumni were compromised in database breached by hacker. The hacker took names, Social Security numbers, dates of birth and university identification numbers even though the database protected with "multi-layered security defenses [12].

A study of 36 universities in the United States also found that IHLs had suffered from 319 attacks on their information resources [4]. On the other hand, in another study conducted in 2006 on information security in higher education, 124 of 182 participants specified that their institutions had experienced at least one information security breach in 2005 [5]. While, in June 2003 a computer virus at Stanford University broadcasted confidential employee salary and bonus information to about 35,000 Stanford users [6]. Similarly, in February 2003, an intruder accessed names and social security numbers of 59,000 students, faculty, and staff at the University of Texas at Austin [6]. All these show that IHL's needs to protect her confidential information from being intruded.

The objectives of Malaysia's higher education system are:

Proc. of the Second Intl. Conf. on Advances in Computing, Electronics and Electrical Technology - CEET 2014.

ISBN: 978-1-63248-034-7 doi: 10.15224/ 978-1-63248-034-7-29

a. To promote national integration and unity
b. To meet the high-level manpower requirements of the country
c. To build a progressive society, oriented towards modern science and technology

In order to produce high-level manpower requirement, the student and staff need to be educated about the importance of information security knowledge to protect national, organizational and individual confidential data. This is because the security concerns are evolving alongside with the development of technology. IHL such as UNISEL is entrusted with confidential information regarding their students, staff, finance and alumni. Institutions of higher education must protect this information because the cost of insecurity can be very high [22].

The examples of incidents of security breach occurrence taking place at IHL's are institutions' computer system being hacked or attacked by viruses or worm, malicious software infections, and infiltration of other entities via their networks. The adverse impacts of these incidents include compromised private data and intellectual property, substantial financial losses, and potential threats to critical infrastructure, public safety, and national security. Thus, the computer and information had been incorporated as part of the institutions activities, and programs are a need to be secured.

III. Methodology

The study is undertaken to report on the Information Security awareness and practice by this specific target group of staff at Faculty of Computer Science and Information Technology (FCSIT), Universiti Selangor (UNISEL). The groups selected for the study are taken from two different job classifications in FCSIT.

This survey instrument, a questionnaire that was specifically used in this study, is a modified version of the Information Security Awareness (ISA) measurement instrument developed by [23]. The ISA measurement instrument is comprised of a user information security awareness scale, an information security practice scale, a personal innovativeness scale, and a computer self-efficacy scale.

The questionnaire was divided into three sections. The first section consists of demographic questions that inquired about the participant's gender, job classification status, age, and the number of years of computer use. The next two sections were on the user information security awareness scale and information security practice scale. The questionnaires were distributed among the selected FCSIT staff.

Data collections were analyzed based on the Rasch Model for dichotomous data using a computer application, *Bond&FoxSteps* [24]. In addition, the data were also analyzed using SPSS version 17.

Once the questionnaires were distributed, the data was collected from among FCSIT staff i.e. academician, and administrative that represents various departments. Data was gathered from a random sample using the printed questionnaires. The printed survey instrument was used to collect self-reported data from the faculty staffs. Surveys are suitable for collecting self-reported data about the participants' beliefs or behaviors [25]. In addition, the survey research is an appropriate method for this study since it was designed to describe a population [26].

The data was analyzed using Rasch Analysis and SPSS after receiving feedback from respective respondents. Statistical methods were used to summarize or describe a collection of data. This research used Descriptive Statistics for describing the results. For the data reliability, it was analyzed using Reliability Analysis.

Once the data has been collected and analyzed, any patterns that emerge was identified. This pattern will be a guideline to give meaning to or interpret the data in an appropriate way to ensure that the objectives of this research have been achieved.

Through this phase, all data had been documented by following the university format. This is to ensure the understandable of data presentation as well as can be used as a reference in the future.

IV. Results and Discussion

A total of 30 out of 60 (50%) respondent responses to 60 questionnaires distributed to Faculty of Computer Science and Information Technology staff. The outcome of the survey will provide a measure of awareness and practice in information security established reflected by the Person Mean, μPERSON being the Maximum Likelihood Estimate (MLE) in Rasch Analysis.

The survey's reliability and validity have been established through a face validity check, a pretest, a pilot test (N=286—business students—72% return rate) and a factor analysis of the results from the full administration of the survey (N=531 out of 4,938 sampled) by Ryan. The alpha coefficients for each construct were above .80 [23]. The survey for this study was adopted and modified information security awareness and information awareness practice scales by [27].

Based on Rasch Model a total of 690 data points arising from 30 respondents on 24 items was analyzed. It yields a Chi-Square value of 1123.36 with 636 degrees of freedom. The test raw scores of Cronbach-α register a reliability of 0.73 (confident level or error free margin). This allows further analysis of the instrument in measuring the awareness and practices in information security.

Figure 1: Respondent job classification

The demographic analysis shows that 50 percent of respondent are female, and 50 percent of respondent are male. This shows that the percentage of respondent between male and female are equal. Figure 1 shows that 80 percent of the respondents are academician, and the other 20 percent are

Proc. of the Second Intl. Conf. on Advances in Computing, Electronics and Electrical Technology - CEET 2014.

ISBN: 978-1-63248-034-7 doi: 10.15224/ 978-1-63248-034-7-29

administration staff. In term of gender among academician, 54 percent of the academician are female, and 46 percent of the academician are male.

The demographic survey result also shows that 23 percent of the respondents are from category 2 (20-30 years old), 66 percent from category 3 (31-40 years old) and 10 percent from category 4 (41-50 years old). There are no respondents are from category 1 (below 20) and category 5 (over 51). This result shows that most of the respondents are of category three which is their age is between 31 to 40 years old. It shows that most of the respondents are considered to be young which is below 40 years old.

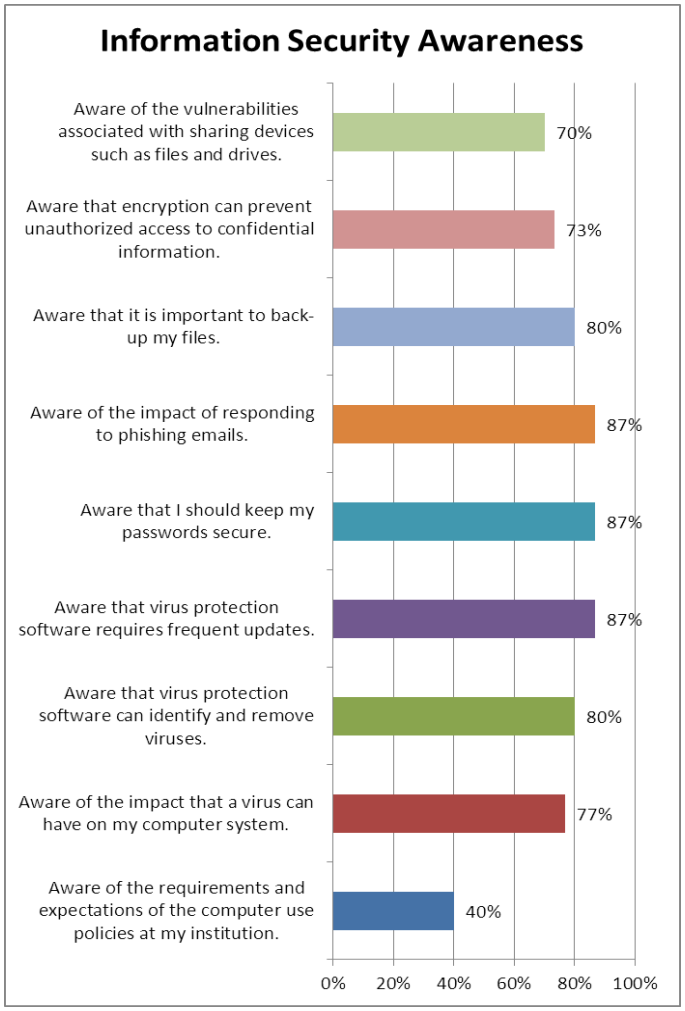

Figure 2: Information security awareness among faculty staff

Figure 2 shows the trend and level of information security awareness among faculty staff. In term of awareness of backup files, keeping password secure, phishing email impact, virus protection software and update virus protection software, 80-100 percent respondents they are aware of this security measure. Next, however, the awareness levels fall onto the average value (51-79 percent) in awareness of virus impact on computer, vulnerabilities of sharing devices and encryption of confidential files information. Lastly, the level of awareness is low (<50 percent) in understanding the requirement and expectation of computer use policies in the institution. This shows that requirement and expectations of the computer use policies among faculty staffs are still low of concern.

The result of the study analysis shows that the lowest mean score is for the item - computer use policies which were 3.17. Nevertheless, the overall score indicated that the average mean of information security awareness score with mean = 3.67 is considered to be significant. That is mean the level of respondent's awareness are good.

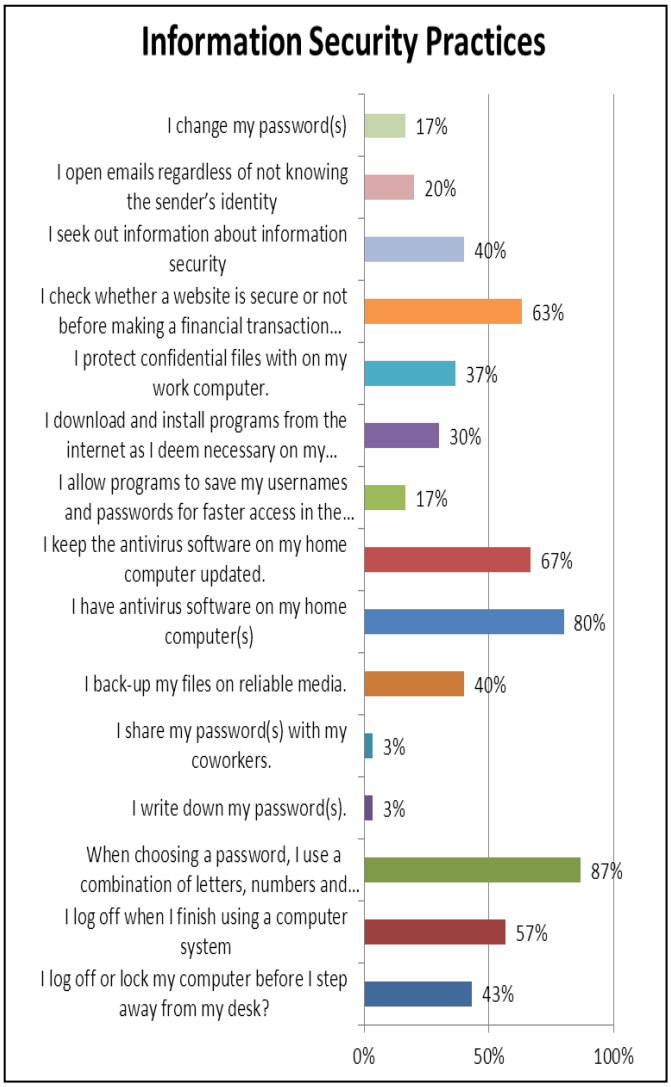

Figure 3: Information security practices among faculty staff

Figure 3 shows the information security practices among faculty staff. The study shows that the level of information security practices is lower as compared to the level of information security awareness. Figure 3 shows the trend and level of information security practices among faculty staff are high (80-100%) in term of choosing password and having

Proc. of the Second Intl. Conf. on Advances in Computing, Electronics and Electrical Technology - CEET 2014.

ISBN: 978-1-63248-034-7 doi: 10.15224/ 978-1-63248-034-7-29

antivirus software installed. For the practice of not writing down the password somewhere and not sharing the password with anyone, the percentage is low. However, it is consider good information security practices. The information security practices levels of the faculty staff are average (51-79%) in checking website security, update antivirus and log off after using computer systems. The survey results show level of information security practices is low (<50%) in many area such as protect confidential files with password, log off after step away from desk, backup files, open emails regardless not knowing the sender, change password and seek information about information security.

The result indicated that the average mean of information security practice score (M = 2.91). This mean level of respondent's practice is fair, and the respondent need more training in information security to upgrade their knowledge on good information security practice. The university must also provide them with good information security guidelines and policies.

v. Conclusion

The study findings show that faculty staffs are aware of information security issues and safe computing practices. However, they do not always practice safe computing behaviors to the same extent as they are aware. The password management continues to challenge the users and IT departments since with good password management system in place; this could prevent unauthorized access to passwords and the vital information. On the other hand, the security applications such as antivirus programs have been made compulsory in managing malware risks since this software can easily attack the computer systems in the IHL. Users should be made known of the damage the malware could cause in terms of cost and university day to day operations. Further, the faculty staff needs to learn on how to deal with phishing e-mails situation. Staff should be more cautious on any emails that direct them to ask for confidential information. However, phishing attempts continued to be a challenge as the hackers were becoming more sophisticated in their attempts. From this study, it is recommended that the Faculty of Computer Science and Information Technology (FCSIT) or Centre for Information, Communication & Technology (CICT) to produce and enforce information security policies. Besides that, they also need to conduct a training to upgrade their staffs security awareness and practice.

This study suggests the Malaysian IHLs information security policy is to be developed to ensure that the academic communities understood the potential risks of information security posed by staff at their academic institutions. The information security policy should include information security standard and computer-related tasks that impact data security. The examples of computer-related tasks that impact data security are password management, data storage devices and documents dispose process, back-up data, comply with the good practice, contend with malware, and manage phishing e-mails.

References

[1] Vishal, B. and Sanur, S., "Data mining: a necessity for information security," Journal of Knowledge Management Practice, vol. 13, no. 1, March 2012.

[2] Christos D.K., "Information from a business perspective: a lottery sector case studies," ISACA Journal, vol 1, 2011.

[3] Ajit, A. and Eric, M. J., "Information security and privacy in healthcare: Current state of research". International Journal. Internet and Enterprise Management, vol. 6, no. 4, 2010.

[4] Young, J. R., "User error, not hackers, is top source of campus computer problems, survey finds [Electronic Version]. The Chronicle of Higher Education," A36, November 2005.

[5] **CDW**-G Higher Education IT Security Report Card, 2006.

[6] Kvavik, R.B., and Voloudakis, J., (with Caruso J.B., Katz, R.N, King, P.& Pirani, J.A."Information technology security: governance, strategy,and practice in higher education. Research Study," vol 5, Boulder, CO;EDUCAUSE Cente fo Applied Research, 2003.

[7] Smith, J. and Frisby, J., "A five-step plan for comprehensive information security and privacy," Bank Accounting and Finance, vol 17, pp31-37, 2004.

[8] Sharma, A. and Ojha, V., "Implementation of cryptography for privacy preserving data mining," International Journal of Database Management Systems (IJDMS), vol. 2 (3), pp.57-65, August 2010.

[9] O'Regan, G., "A brief history of computing," Springer, 2008.

[10] Dlamini, M.T., Eloff, J.H.P., Eloff, M.M., "Information security: The moving target. Computers & Security," In Press. 2008.

[11] Chen, C.C., Shaw, R.S., Yang, S.C., "Mitigating information security risks by increasing user security awareness: a case study of an information security awareness system," Information Technology Learning and Performance Journal.vol 24, pp1-14,2006.

[12] Collin, C., "More than 309,000 identities exposed in University of Maryland cyber attack," Baltimore Sun. 20 Februari 2014.[www document].http://www.baltimoresun.com/news/maryland/bs-md-university-of-maryland-data-breach-20140219-story.html#page=1

[13] Mathew, J.S., "10 biggest information security stories of 2012," Dark Reading.[www document].http:// http://www.darkreading.com/attacks-and-breaches/10-biggest-information-security-stories-of-2012/d/d-id/1107946?

[14] Ashish A., Anand N., and Rahul T.," Does information security attack frequency increase with vulnerability disclosure? An empirical analysis" Information System Front. Springer Science. 2006.

[15] Michael, E.W., "Enemy at the gate:threats to information security" Communication of the ACM, vol 46, no 8, August 2003.

[16] V Conklin, W. A., White, G. B., Cothren, C., Williams, D., & Davis, R. L., "Principles of computer security: security+ and beyond," Boston: McGraw-Hill. 2004.

[17] Bishop, M., "Introduction to computer security." Boston: Pearson. 2005.

[18] Thomson, M.E., and von Solms, R., "Information security awareness: educating your users effectively," Information Management & Computer Security, vol. 6, no.: 4, pp.167 – 173, 1998.

[19] Siponen, M.T., "A conceptual foundation for organizational information security awareness,". Information Management & Computer Security. vol 8, no1, pp31-41,.2000.

[20] Furnell, S.M., Bryant, P., Phippen, A.D., "Assessing the security perceptions of personal Internet users," Computers & Security, 26 (5): 410 – 417, 2007.

[21] Rick,D., "Why universities are under attack by hackers," The Fox News. 11 April 2014. [www document]. http:// www.foxnews.com/ opinion/2014/04/11/why-universities-are-under-attack-by-hackers/

[22] Foster, K.J., "Perimeter security technology development," CIP Perimeter Security Workshop, Canberra, 2004.

[23] Ryan, J. E., "A comparison of information security trends between formal and informal environments,". Retrieved from ProQuest Digital Dissertations database. (Publication No. AAT 3225287). 2006.

ISBN: 978-1-63248-034-7 doi: 10.15224/ 978-1-63248-034-7-29

[24] Trevor, B. & Christine, F., "Applying the rasch model: fundamental measurement in the human sciences," Mahwah NJ: Lawrence Erlbaum Associates, 2001.

[25] Neuman, W. L.. "Social Research Methods, Qualitative and Quantitative Approaches", 5th Edition. Boston: Allyn and Bacon. 263-303. 2003.

[26] Babbie, E. R. "The Practice of Social Research", 9th edition. Wadsworth Pub Co.2000.

[27] Chwiraidzo, J.N. "An Analysis of Perceived Faculty and Staf Computing Behaviors That Protect or Expose Them or Others to Information Security Attack". East State Tennessee University.Theses. 2008.

About Author (s):

"Faculty staffs are aware of information security issues and safe computing practices although they do not always practice safe computing behaviors to the same extent as they are aware"

"University must take precaution steps to encounter cyber-attack"

"Universities data are very valuable assets. It needs to be secured…"

"Inadequate security awareness of user can contribute to information security attack"

"Cyber-attack are increasing day by day"