Information Security Behaviour: A descriptive analysis on a Malaysian Public University.

Ramlah Hussein
School of Computer Technology
Sunway University
Selangor, Malaysia
ramlahh@sunway.edu.my

Fateema Lambensa
Kulliyyah of ICT
International Islamic University Malaysia
Kuala Lumpur, Malaysia
nongmah@yahoo.com

Raja Baharuddin Anom
Department of Information Systems
Advanced Informatics School
Universiti Teknologi Malaysia
rbahar@ic.utm.my

Abstract- The critical issues of information security have gradually increased. Effective information security management require a great understanding both technological and human dimensions. Thus, the purpose of this research is to investigate the university student's behavior towards information security and to examine factors influencing information security behavior. The study adopted the quantitative approach by conducting a survey among students in one of the public universities in Malaysia. Questionnaires were distributed to the targeted respondents. Then, the SPSS software was used to systematically analyze all data obtained and generate statistical information and detailed analyses of the survey results. This study is helpful in exploring issues related to information security behavior. Hopefully, this study contributed to an understanding of the influencing factors towards the university students' behavior in relation to information security.

Keywords: *Information Security, Security Threat, Information Security Behavior, Self-efficacy, Perceived Importance*

I. INTRODUCTION

With more than one billion people connected to the Internet worldwide, it has had a revolutionary impact on how people learn, interact, and communicate [1]. The rapid growth in computing and networking technologies has become a part of student life. Internet provides students quick access to a large number of information sources. Yet, along with these sources, the Web contains millions of other websites managed by individuals, businesses, advocacy groups, clubs, and so on, which may offer inaccurate or biased information [2]. Students regularly access through Internet not only for their academic purposes but also for personal purposes. Students may not be aware to protect their computers from security attacks while they are browsing the Internet.

Keeping computers secured is becoming increasingly difficult. Attacks by computer viruses, spyware, and security breaches in computer systems are almost daily occurrences. These incidents have serious effects on various aspects including academia. A recent report, "Breaches in the Academia Sector", by John Correlli of JMC Privacy Consulting Group [3], noted that from 2005 through 2007, there were 277 widely reported breaches at colleges and universities in the United States. Furthermore, the 263 reported privacy data breaches in the United States in 2008, about one-third occurred at colleges and universities [4].

The development of information security remains a difficult process to protect personal and sensitive information from security attacks. Numerous sophisticated security methods have been developed, but information security is declining [5]. No matter how well designed, security methods rely on individuals to implement and use them. Technological solutions are important but not sufficient [6]. The success of security also depends on the effective behavior of individuals [7, 8].

The threats to information security can influence IT users' perception and behavior [9]. Therefore, it is essential for a better understanding of IT users' attitude and behavior on what they perceive, why they perceive it, and how they will subsequently behave in information security [9]. Thus, the study aims to investigate the university student's behavior towards information security and to examine factors influencing information security behavior in a public university in Malaysia.

II. LITERATURE REVIEW

Information Security

Information security is a socio-technological problem which requires thorough understanding of the weakest link in the defense against security threats: human behavior and attitudes about using these security technologies [10, 11, 12]. According to an official definition, information security is the protection of information and the systems and hardware that use, store and transmit that information [13]. From the technical point of view, information security aims to protect the availability, accuracy, authenticity, confidentiality, integrity, utility and possession of the information [14].

Behavioral Information Security

The behavioral information security is defined as the complexes of human action that influence the availability, confidentiality, and integrity of information systems [15]. Advancements in IT have often created new opportunities for use and risks for misuse of personal information. Information security can be managed through three separate mechanisms which are people, policy and technology [16]. With respect of information security in academic setting, Cox, Connolly and Currall claimed that security makes requirements not only good technical solutions but also effective behavioral users [7]. Indeed, a key component of computer systems is the end user.

LaRose, Rifon, Liu and Lee further explained the criterion of protective behaviors in online safety domain such as updating operating system and browser patches, updating virus protections, deleting cookies, and changing passwords [17]. Users' behavior is critical to information security. There needs to be a security culture among users. The actions of end users play a significant role in the achievement of securing computer environment. There are multiple security mechanisms that need to be engaged and updated in securing computer operations. Users have to make responsible decisions with security implications, for example keeping their virus files up to date, updating software and treating email attachments with caution, in order to provide as a background service with a security risk attached [7].

Attitude

Attitude has been proposed to influence behavioral intentions in multiple theories, such as the TPB [18] and the TRA [19]. According to Ajzen and Fishbein [20], attitude towards the behavior is defined as a person's general feeling of favorableness or unfavorableness for that behavior. Attitudes are informed by beliefs and norms are informed by normative beliefs as well as motivation to comply [18]. Importantly, attitudes affecting intentions are the perceived desirability of the outcome to the individual.

Generally, the more favorable a person's attitude is towards behavior, the more likely it is that the person will want to engage in the behavior. As a result, attitude towards a specific information technology is conceptualized as a potential user's assessment of the desirability of using that technology [21].

Information Security Self-efficacy

Research investigating computer use and behaviors has often utilized the construct of self-efficacy, derived from Bandura's Social Cognitive Theory. The concept of TPB's perceived behavioral control is close to the concept of self-efficacy of Bandura [22]. According to Bandura [23], self-efficacy as a major cognitive force guiding individual behavior in this reciprocal relationship among environment, behavior and individual. He defined self-efficacy as people's judgment of their capabilities to perform a task. Self-efficacy is concerned with judgments of what one can do with whatever skills one possesses and not with skills. The most powerful of self-efficacy is the interpreted result of one's own previous attainments, or mastery experience.

Self-efficacy has been shown to influence choice of whether to engage in a task, the effort expended in performing it, and the persistence shown in accomplishing it [24]. People who have higher level of self-efficacy towards a specific subject are more like to give greater value to that subject. In the context of IT, the research suggested that individual who possesses high self-efficacy towards IT, use IT more frequently [25]. Previous studies have shown the relationship between self-efficacy and behavior [26, 27].

Perceived Importance

Perceived importance is defined as the degree to which an individual perceives a certain event or behavior to be important [28]. It has been discussed in various studies as one of the factors driving individual motivation to perform behavior. For instance, Pajares and Graham [29] examined the middle school students who have high performance in mathematics have high perceived importance of mathematics. In evaluating training programs, employee's perceived importance of the training program plays an essential role in rising motivation to join and do well in the training program [30].

Information Security Experience

Users who have experienced or have close knowledge of someone's experience in a significant loss as a result of a security issue will likely remember the event and use it when examining future possibilities [31]. Previous experience offer the user a unique perspective associated with the subject. Jaw and Chen stated that students who know more about Internet security techniques are likely to be more aware of Internet security threats [32].

III. METHODOLOGY

The study applied a quantitative approach applying a survey research design in form of questionnaire as the data collection strategy in order to achieve its objectives and to answer the research questions posted in the study. Respondents consist of students from a public university in Malaysia and only respondents who have either PC or laptop are allowed to take part in the survey. A self-administered questionnaire was designed to capture the data of study. A total number of 180 questionnaires were distributed to target respondents from seven faculties.174 questionnaires were collected and 160 were usable for the study because they met the criteria of having no missing data or uncompleted data. This study applied measures that have been validated in previous research to ensure the control of measurement errors. However, the adopted measures are modified to reflect the context of information security. Information security behavior was measured by using an instrument from previous study [33, 34]. The instrument for attitude has been adapted from Ng and Rahim [35] and conklin [31]. Self-efficacy measures were adapted from self-efficacy literatures with respect to information security [31, 35]. Perceived importance measures were adapted from the exploratory study [38]. A seven-point Likert scale was used to measure the level of agreement to the statements ranging from 1 (Strongly Disagree) to 7 (Strongly Agree). However, information security experience was measured in term of novice/beginner, intermediate, or advanced. The study used Statistical Package for the Social Sciences (SPSS) version 16.0 to describe and analyse the data. Descriptive statistics were used to summarize and simplify data.

IV. RESULTS

Respondent Profile

The majority of the respondents are female with 60% while 40% are male. Respondents with the age between 20-22 years have the highest percentage of 46.9%, followed by those with age between 23-25 years which accounted for 30.6% while the remaining of respondents are age of 26-28 (10.6%), 28 and above (9.4%), and below 20 (2.5%) respectively. Slightly more than half of the respondents are undergraduate students (72.5%) and the remaining are postgraduate students (27.5%).

Reliability Test

The reliability analysis was conducted to ensure the internal consistency of the items used for each variable. Cronbach's alpha calculations were made to determine the level of internal consistency within each construct. Cronbach's alpha score generally agreed upon lower limit is 0.70 [36]. The result shows values of Cronbach's Alpha are higher than 0.70 indicating that all the constructs are reliable and suitable to measure the concepts employed in the study.

Internet Experience

The information about respondents' computer and Internet experiences were also collected through the questionnaire in term of length of period, duration of computer and Internet use, level of computer and Internet experience as well as level of information security experience. The highest percentage of respondents (35.6%) have computer and Internet experience between 3 to 4 years followed by those who have experience between 5 to 6 years (26.9%), more than 6 years (23.8%), 1 to 2 years (11.2%) and less than 1 year (2.5%) respectively. Furthermore, most of respondents used computer and Internet for a minimum of 5 to 6 hours a day accounted for 48.8% and 20.6% were found to use between 3 to 4 hours while 13.1% were respondents who used 7 to 8 hours and 11.2% used computer and Internet for 1-2 hours. Only 6.2% of the respondents used computer and Internet more than 8 hours. Majority of the respondents (83.1%) are intermediate users and the remaining were advanced users (13.8%) and novice/beginner users (3.1%) in term of computer and Internet skills.

Table 1 : Internet Activities

ITEM	**Frequency (%)**	**Frequency (%)**
Internet Activities	***YES***	***NO***
Downloading software	116(72.5%)	44(27.5%)
Online shopping	53(33.1%)	107(66.9%)
Research	154(96.2%)	6(3.8%)
News	152(95.0%)	8(5.0%)
Online games	96(60.0%)	64(40.0%)
Product and service information	119(74.4%)	41(25.6%)
Entertainment	146(91.2%)	14(8.8%)
Education (electronic papers, etc.)	151(94.4%)	9(5.6%)
E-mail	160(100%)	-
Chat room	120(75.0%)	40(25.0%)

As shown in Table1, the results indicates that all respondents have used the Internet for e-mail services (100%), research purposes (96.2%), reading online news (95%), downloading electronic papers (94.4%) and entertainment (91.2%). However, only 75%, 74.4%, 72.5%, 60.0% of the respondents used the Internet for chatting, gathering product and service information, downloading software, playing online games respectively. Only 33.1% of the respondents have conducted purchase over the Internet. This result can be implied that most of students access the Internet not only for educational purposes but also for other personal purposes.

Attitude

There are four items used to measure attitude factor. The mean of attitude factor ranged from 5.92 to 6.30 indicates that respondents positively agreed to all items given on attitude factor. The attitude construct covers a wide array of potential issues associated with information security that impact the operational aspect of a computer's use. This study uses antivirus software, operating system patches, backups and the use of passwords as measures of operational security posture. The general mean score of 6.1 indicates that respondents tend to have positive attitude towards information security practices in secure manner such as updating antivirus software, updating security patches for operating system or computer program, creating backup critical data and password management.

Information Security Self-efficacy

The study used four items to evaluate the Information Security Self-efficacy factor. The mean ranged between 4.8 to 5.59. The result implied that respondents fairly believed on their skills or abilities in protecting security breaches as well as practicing information security. However, respondents agreed that they have sufficient capabilities in updating antivirus software even there was no one around to help them. Antivirus software is usually configured to start automatically update database when users access to the Internet. Thus, respondents would feel comfortable updating antivirus software. In general, respondents rather believe in their own abilities to practise information security in secure behaviour with an overall mean score of 5.25.

Perceived Information Security Importance

The perceived importance of information security consisting of four items were also measured. The mean range of perceived information security importance is between 6.03 and 6.42.The results shows that the respondents agreed to all questions given for the perceived importance of information security construct. They tend to have high perceived importance of information security such as protecting computers from security breaches and keeping personal information private during Internet use. The overall mean score of the construct is 6.17 which can be implied that respondents generally have strong perceived importance of information security and thus they may have more motivation to be more proactive in their information security behaviour.

Information Security Behaviour

Measuring the security behaviour should take into account of the various security measures available. For this study, six items from previous studies as mentioned in the earlier chapter were used to evaluate aspects of information security behaviour. The mean ranged from 4.99 to 5.84. These reflect that respondents agreed to practice information security by paying attention and updating antivirus on a regular basis including not sharing password with others. However, the results also indicates that respondents somewhat agreed to update security patches for their operating system (OS)/computer program, make backup critical data as well as exercise caution with their password. Antivirus programs provide protection from specific security threats such as viruses and worms. Running regular update to the antivirus application is requires in order to maintain a proper security in identifying and protecting from security threats. Students can easily perform automatically update to antivirus software when they access through Internet.

Security threats usually attack computers linked to the Internet by looking at vulnerabilities or errors found in the systems. OS and/or application software can maintain through a series of patches after newly discovered vulnerabilities or weaknesses in existing OS or software. The issue of obtaining and applying the patch requires the specific level of student's effort to install the patches may vary, from automated download and patch management.

Backup is also one of the recommended security practices against data loss in the event of system failure. Password is additionally information security measures being applied to a personal computer as well as online account to prevent unauthorized access to information. Appropriate use of passwords to protect systems and information is the initial elements of system security. A criterion can concern the construction and use of passwords. For instance, password might have a certain length (e.g. eight characters) and a certain composition (e.g. consist both of lowercase and uppercase as well as special characters such as '/', '#' and '@').

The entire mean score of information security behaviour is 5.39 Therefore, this is likely that students demonstrate to activate security protection behavior such as updating antivirus on regular basis, paying attention to antivirus database updates or operating systems updates when surfing Internet, using strong password for computers as well as e-mail account and not sharing password with other people in order to protect their private information. Moreover, the study also found that student's level of expertise on information security has a significant impact on information security behavior. Students who have high skills or knowledge in information security issues concern for their information security and privacy more than those who have lower skills. Advanced users were able to manage when their computers are infected by security threats. They are more likely to protect their computer and exercise care when perform tasks over Internet such as downloading the file or software from the Internet as it may contain viruses.

V. CONCLUSION

Information security require a great understanding both technological and human dimensions. Information security threats could be minimized if users performed effectively information security behavior. The success of information security depends on the effective behavior of the individuals involved in its use. The study has examined behavioral information security perspective in the context of university students as users and established factors which are significant to the student behaviors towards information security. The result of this study is hoped to contribute in developing an understanding of important factors influencing behavior of university students towards information security. This would lead to organize more information security awareness programs to promote privacy and security protection behaviors. Information security awareness programs are important approach but such programs have to be effective in influencing user's information security behavior.

REFERENCES

[1] Ciampa, M. (2007). *Security awareness: Applying practical security in your world* (2nd ed.). Massachusetts: Course Technology, Thomson Learning.

[2] Metzgera, M., Flanagina, A. J., & Zwarun, L. (2003). College student Web use, perceptions of information credibility, and verification behavior. *Computers & Education, 41*, 271-290.

[3] Correlli, J. (2009). *Breaches in the Academia Sector*. (JMC Privacy Consulting Group) Retrieved August 12, 2009, from http://jmcconsulting.wptlite.com/getdownload.asp?id=595

[4] Claburn, T. (2009, March 17). *Binghamton Data Breach Threatens CISO's Position*. Retrieved August 12, 2009, from http://www.informationweek.com/news/security/attacks/showArticle.jhtml?articleID=215900749

[5] Turner, D., Entwisle, S., Fossi, M., Blackbird, J., McKinney, D., Conneff, T., et al. (2006). *Symantec Internet security threat report – trends for January 06 to June 06*. Retrieved July 17, 2009, from http://www.symantec.com

[6] Rhodes, K. (2001). Operations security awareness: The mind has no firewall. *Computer Security Journal, 18* (3).

[7] Cox, A., Connolly, S., & Currall, J. (2001). Raising IS security awareness in the academic setting. *VINE, 123*, 11-16.

[8] Stanton, J. M., Mastrangelo, P. R., Stam, K. R., & Jolton, J. (2004). Behavioral information security: Two end user survey studies of motivation and security practices. *Proceedings of the Tenth America's Conference on Information Systems* .

[9] Huang, D. L., Rau, P. L., & Salvendy, G. (2008). Perception of information security. *Behaviour & Information Technology*, 1-12.

[10] Goodhue, D., & Straub, D. (1991). Security concerns of system users: A study of perceptions of the adequacy of security. *Information & Management, 20*, 13-27.

[11] Dhillon, G., & Backhouse, J. (2001). Current direction in IS security research: Towards socio-organizational perspectives. *Information Systems Journal, 11*, 127-153.

[12] Hu, Q., Hart, P., & Cooke, D. (2006). The role of external influences on organizational information security practices: An institutional perspective. *Proceedings of the 39th Hawaii International Conference on Systems Science (HICSS 39)*, (pp. 1-10). Hawaii, USA, January 4-7 2006.

[13] National Institute of Standards and Technology [NIST]. (1995). *An introduction to computer security: The NIST handbook.* Special Publication.

[14] Whitman, M. E., & Mattford, H. J. (2004). *Principles of information security.* Thomson Learning.

[15] Stanton, J. M., Caldera, C., Isaac, A., Stam, K. R., & Marcinkowski, S. J. (April, 2003). Behavioral information security: Defining the criterion space. In P. M. Mastrangelo, & W. Everton, *The Internet at work or not: Preventing computer deviance.* Orlando, FL.

[16] Penn, J. (2006). *Aligning data protection priorities with risks.* Forrester Research.

[17] LaRose, R., Rifon, N., Liu, X., & Lee, D. (2005). Understanding online safety behavior: A multivariate model. *International Communication Association.* New York.

[18] Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, 179-211.

[19] Fishbein, M., & Ajzen, I. (1975). *Belief, attitude, intention and behavior: An introduction to theory and research, reading.* MA: Addison-Wesley.

[20] Ajzen, I., & Fishbein, M. (1980). *Understading attitude and predicting social behavior.* Englewood Cliffs, NJ: Prentice-Hall.

[21] Davis, F., Bagozzi, R., & Warshaw, P. R. (1989). User acceptance of computer technology: A comparison of two theoretical models. *Manage Science, 35* (8), 982-1003.

[22] Bandura, A. (1982). Self-efficacy mechanism in human agency. *American Psychologist, 37* (2), 122-147.

[23] Bandura, A. (1986). *Social foundations of thought and action.* New Jersey: Prentice Hall.

[24] Bouffard-Bouchard, T. (1990). Influence of self-efficacy on performance in a cognitive task. *The Journal of Social Psychology, 130*, 353-363.

[25 Compeau, D., Higgins, C. A., & Huff, S. (1999). Social cognitive theory and individual reactions to computing technology: A longitudinal study. *MIS Quarterly, 23* (2), pp. 145-158.

[26] Bandura, A. (1977). Self-efficacy: Toward a unifying theory of behavioral change. *Psychological Review, 84*, 191-215.

[27] Chambliss, C., & Murray, E. (1979). Cognitive procedures for smoking reduction: Symptom attribution versus efficacy attribution. *Cognitive Therapy and Research, 3* (1), 91-95.

[28] Chai, S. (2009). *Three essays on behavioral aspects of information systems: Issues of information assurance and online privacy.* PhD Dissertation, Department of Management Science and Systems, School of Management, State University of New York.

[29] Pajares, F., & Graham, L. (1999). Self-efficacy, motivation constructs, and mathematics performance of entering middle school students. *Contemporary Educational Psychology, 24*, 124–139.

[30] Tsai, W., & Tai, W. T. (2003). Perceived importance as a mediator of the relationship between training assignment and training motivation. *Personnel Review , 32* (1/2), 151-163.

[31] Conklin, W. A. (2006). *Computer security behaviors of home computer users: A diffusion of innovation approach.* PhD Dissertation, University of Texas, San Antonio.

[32] Jaw, G. Y., & Chen, J. Y. (2007). Asian new generation's perceptions regarding network fraud. *Second International Conference on Innovative Computing, Informatio and Control (ICICIC 2007).* Kumamoto, Japan.

[33] Boss, S. R. (2007). *Control, perceived risk and information security precautions: External and internal motivations for security behavior.* PhD Dissertation, University of Pitttsburgh, Faculty of the Joseph M. Katz Graduate School of Business.

[34] Galvez, S. M., & Guzman, I. R. (2009). Identifying factors that influence corporate information security behavior. *Proceedings of the Fifteenth Americas Conference on Information Systems*, (pp. 1-11). San Francisco, California, August 6th-9th 2009.

[35] Ng, B. Y., & Rahim, M. A . (2005). A socio-behavioral study of home computer user's intention to practice security. *The Ninth Pacific Asia Conference on Information Systems*, (pp. 234-247).

[36] Hair, J. F., Anderson, R., Tatham, R. L., & Black, W. (1998). *Multivariate Data Analysis* (5th ed.). Englewood Cliffs, New Jersey: Prentice Hall.