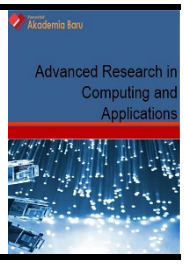
Penerbit Akademia Baru

Journal of Advanced Research in Computing and Applications

Journal homepage: www.akademiabaru.com/arca.html
ISSN: 2462-1927



The awareness of security breach among IT users in Kolej PolyTech MARA, Batu Pahat

Open Access

Intan Safina Othman [1,*], Abdul Samad Shibgatullah [1], Abd. Samad Hassan Basari [1], Zul Azri Muhammad Noh [1]

[1] Faculty of Information and Communication Technology Universiti Teknikal Malaysia, Hang Tuah Jaya, 76100 Durian Tunggal, Melaka, Malaysia

ARTICLE INFO

Article history:
Received 31 July 2016
Received in revised form 17 November 2016
Accepted 20 November 2016
Available online 9 December 2016

ABSTRACT

Recently, network security has become a major concern in cyber world. Thus, the need for cyber security is higher in order to ensure data safety and privacy. The internet is widely used in internet banking, online shopping, data storage, global positioning system, media and many other social applications. Security has become a critical aspect in an overall information security area. Human error inadvertently causes security breaches if the user fails to practice safety behavior. This study was conducted to investigate the factors contributed by individuals and organization on information on security awareness towards security breach among IT users in Kolej Poly-Tech MARA Batu Pahat (KPTM BP). By observing the literature review and related research, this study proposed a research model of the awareness of security breach by relying on the individual, organization and information security awareness. In conjunction with the proposed model, this study addresses 2 hypotheses which are; H1- there is no relationship between independent variables and dependent variables; H2- there is a relationship between independent variables and dependent variables. The descriptive research has been used to investigate the awareness of information security focusing on human error, policies and procedures and information security awareness in education and experience via questionnaires. The respondents of this study comprise of 155 IT users in KPTM that used snowball sampling to gather data. This study can be used to assist the IT Officer in Batu Pahat and others branches in KPTM to monitor the awareness level of users towards information security, thus enabling them to design an effective information security awareness programs such as campaign, seminar and case study. Meanwhile, KPTM, Batu Pahat, can also utilise this study to design a more robust system of policies and procedures that would safeguard the confidentiality, integrity and availability of the system. For future work, this study can be implemented in other private and public colleagues and universities to cover a larger population for the purpose of sampling.

Keywords:
Security breach, Network security, KPTM BP

[*] *Corresponding author.*
E-mail address: intan_safina@gapps.kptm.edu.my (Intan Safina Othman)

1. Introduction

The phrase 'New Tools, Old Crime' is referred to the crime that occurs in cyberspace by using networking devices tools [1]. Nowadays, internet use is widespread. The technology shift has enabled many companies to produce various types of devices such as computers, mobile devices, smart phones, tablets, iPad, and other mobile devices that can connect to the internet anytime and anywhere. The internet provides a lot of advantages to the user including easy access to the social media, online chatting, online purchase, online banking, streaming video, sending and receiving email through the World Wide Web. Although the internet solves many issues regarding technology, at the same time it also creates a host of other problems especially if the user is ignorant regarding the issues of information security [2]. This study focused on the awareness of security breach among IT users in Kolej Poly-Tech MARA Batu Pahat (KPTM BP). The most common error committed by users are; sharing their passwords with another user, opening unknown emails, leaving workstations unattended, updating status on media social, etc. Their carefree attitude towards information security leaves them vulnerable to hackers or attackers to penetrate into the user's system. Once the attacker starts hijacking the system, data confidentiality, availability and privacy can no longer be secured [3]. Moreover, if the organization fails to take a major action aiming at strengthening information security, one of the consequences would be organizational asset loss.

Employees are the biggest contributors in information security breach. Occasionally, their actions may deliberately affect the organization. Examples of user misconducts include employee carelessness, failure to abide by policies and procedure, improper data storing and trainings not conducted by authorized trained personnel. Nevertheless, employees themselves can sometimes employ information assets for personal reasons such as illegal access towards data confidentiality, data fraud, downloading and installing malicious software, misusing data, etc. [4]. According to [5], human error can be categorised into seven focus areas which are information handling, password management, mobile computing, internet use, social networking use, incident reporting and email use. An interview with an IT executive of KPTM Batu Pahat indicated that human error are commonly responsible for information security breach and this view is supported by [5,6]. Thus, the development of the questionnaire is based on the behavior, knowledge and attitude associated with human error in computer usage or application. As users of the Internet, they must be knowledgeable and aware of any kind of activities involving the internet. A user must also bear in mind that everything can be accessed by an attacker every time the user logged on to the internet [7]. Thus, without awareness in cyber security the user will inadvertently provide an opportunity for an attacker to penetrate into his system without his knowledge.

2. Overview of information security awareness, human error and security breach

Information security awareness can be described as the state of consciousness where the user can distinguish the action accordingly, comply with the rules and regulations, and understand the impact of his actions [8]. Without proper understanding in Information Security Awareness, cases like security breach can occur and can impact the organization; therefore, action should be taken to prevent it from occurring. The researchers claimed that each of the individual, institution, and environmental causal must clearly understand their responsibilities when using the internet or computer. According to [9,10], security awareness can be interpreted as an understanding about the network security; policies and procedures; and individual factors. User practice is the major aspect that contributes to the security breach. Online shopping, opening unknown emails and attachments, cloud storage and passwords sharing are examples of user's customary practice on the internet.

Cyber awareness training is an example of a factor that could contribute to security awareness. Nevertheless, the user's actual behavior remains the main factor that contributes to the security awareness [9,10].

Human error can be referred to accidental causes where it denotes the concept of violations: deliberate actions that deviate from normal process. The concept of violations can be divided into two categories: harms of malicious intent (e.g., insider threats, hackers, terrorists) and harms of a non-malicious nature. In this context, human errors and individuals are considered two different entities whereby an individual cannot be blamed if human error occurs [11]. According to [12], intrusions in cyberspace can be categorized as attacks from insiders, flooding intrusions, root attacks, port scanning attacks, attacks on the virtual machines and attacks from back door channels [12]. Human negligence or human error is one of the factors that contribute to cyber-attack [13]. This has been proven through researches done by James Reason. His research claimed that other factors that contribute to human error and violation are misuse of equipment, management not implementing best practices or setting out unclear procedures [14]. Previous studies conducted by [5], stated that human error that most contribute to the destruction of an organization are carelessly or purposely exposing passwords to others, falling victim to phishing emails by clicking on embedded web site links, or installing non-familiar media into work or home computers. Metalidou who examined the relationship between human factor and management factors found that human factors are the major contributor to security breach and this conclusion was supported by [2] and Cisco Systems.

2.1 Previous research model for framework adaptation

Related studies conducted by the researchers about the awareness of security policies towards user acceptance perspective found that the factors that contribute to the security awareness are organization, human and social [15,16]. Moreover, according to [17] on a study conducted on mobile device focusing on smartphone awareness, the researchers claim that behavior, attitude and knowledge are the factors that contribute to the security awareness. Recent study about information security awareness has been deployed and the researchers [18] proved that policy, security, attitude, Subjective Norms, organization, involvement experience, threats appraisal and self-efficacy shows a strong effect on user behavior where the researcher piloted the study in the SEM (structural equation modeling) [18]. Based on empirical researches and theoretical framework, most of the researchers agreed that the factors that contribute to security breaches are individuals, organization and information security awareness [5].

Although an organization has implemented information security, however, policies and procedures alone are not enough to curb information breach that happen in a year according to [19]. Organization factors relating to the implementation of policies and procedures, attitude toward policies and procedures as well as information security culture has been conducted and it is recommended that a user should always adopts best practice behavior when surfing the internet or when using a computer or a laptop. A lot of literatures have used behavior model in information security like the Theory of Planned Behavior [20] and the Knowledge Attitude Behavior (KAB) model [21].

[22] have conducted an analysis to compare the three models behaviour. They are technology acceptance model, combine theory planned behaviour and technology acceptance model and unified theory of acceptance and use of technology. The researchers found that attitude shows a positive result towards user behaviour. Organizations, colleagues are the factors that contribute to employee actions. Moreover, researchers [5] also agree that employee behaviour is the main factor that influences security breaches in term of human error. [5] examined the relationship between factors

of HAIS-Q by using KAB Model. The researchers used knowledge, attitude and behaviour (KAB) model to find the relationship between knowledge toward policy, attitude toward policies and procedures and self-reported behaviour based on human error. They found that individual, organization and information security awareness are the factors that contribute to employee awareness by using HAISQ [5]. This statement was supported by [23] where the researchers conducted empirical study to examine the factors that contribute to information security culture on employee practice. The study has been conducted through various disciplines involving banking, information technology, finance, marketing, education, advertising, engineering and healthcare environment. The result shows nine factors that influence information security culture. They are security behaviour, cultural differences, top management, trust, information sharing, security policy, security knowledge and belief.

3. Methodology

A descriptive research study has been conducted to investigate awareness level towards security breaches focusing on knowledge on policies and procedures; technology and system adapted from Neil J. Salkind's method by using a questionnaire. A questionnaire is used to capture rich, detailed information that contributes to human behavior and knowledge towards policies and procedures in security breach among IT users in KPTM BP. By using a descriptive quantitative research design the detailed information can be gathered to design or adopt an exploratory approach regarding network security issues. The questionnaire was constructed using a hybrid method. The selected populations of this study are from the education sector mainly with knowledge in information technology focusing on KPTM BP. This study took a sample of 30% of KPTM BP users comprising mainly of students and staffs that amounted to 330 respondents from various backgrounds. The result of the interview indicates that there is no documented form of policies and procedures implemented in KPTM BP. Even though network monitoring has been deployed, there is no evidence of any analysis made because the network monitoring was conducted by vendor. Human activity is also a major contributor to the security breach. As regards the information on security awareness program, there has been no security awareness program designed or developed by the IT officer.

4. Result and analysis

This paper starts with collecting and analysing the demographic of respondents of this research survey. Before the questionnaires were distributed to students and staffs, a pilot study was conducted. Cronbach alpha calculated for each of the three main items are: individual, organization and information security awareness. All the items show the recommended cut-off value of 0.7, which provides evidence of a high degree of reliability and suggests the items in the scales are measuring the same underlying construct. The respondents of this research were gathered starting April 2016 until May 2016. From a total of 200 responses, 155 responses were completed and 45 responses were incomplete. The questionnaires were distributed manually using a snowball concept throughout the KPTM BP. The survey was tested over a pilot study to make sure the survey was reliable and understandable. The analysis begins with a descriptive analysis where the demographic of respondents were analyzed using SPSS, followed by survey analysis, where a deeper analysis is done on individual factor, organizational factor and information security awareness. Lastly, independent variables and dependent variables are analyzed using correlation and coefficient, and regression analysis.

Table 1 below summarizes the demographics questions such as age, gender, education level,

which department the staff is working in, the field of study for the student and the length of time spent on the internet and computer. The mean age of the participants is 1.63 (below 20 years); the mean gender is 1.5 (Male); the average for education level is 1.27 (Diploma level); the average for field of study is 3.85 (Graphic Design Programme); the average for working department is 3.57 (Admin Staff) and the average for duration of time experience using the Internet and computer is 3.03 (range 5-10 years).

Table 1
Individual factor frequency

	MIN	MAX	MEAN	MEDIAN	MODE	STD.DEVIATION
AGE	1	5	1.63	1	1	1.075
GENDER	1	2	1.54	2	2	.500
EDUCATION LEVEL	1	3	1.27	1	1	.573
DEPARTMENT	1	4	3.57	4	4	.940
FIELD OF STUDY	1	6	3.85	4	4	1.710
EXPERIENCE USING THE INTERNET AND COMPUTER	1	4	3.03	3	4	.987
TOTAL=160						

Table 2
Individual factor frequency

A	INDIVIDUAL FACTOR	1	%	2	%	3	%	4	%	5	%
IND1	I have sufficent knowledge about information security.	12	**7.74**	34	**21.94**	68	**43.87**	38	**24.52**	3	**1.94**
IND2	I know various types of security threat like malware, virus, botnet and etc	3	**1.94**	14	**9.03**	50	**32.26**	79	**50.97**	9	**5.81**
IND3	I always use a strong password on my computer, email and any social media account.	2	**1.29**	4	**2.58**	32	**20.65**	84	**54.19**	33	**21.29**
IND4	I am not surfing any social networking website or application during class or work time at the college.	3	**1.94**	19	**12.26**	17	**10.97**	56	**36.13**	70	**45.16**
IND5	I always update anti virus programme or anti spyware programme on my computer	2	**1.29**	16	**10.32**	36	**23.23**	40	**25.81**	61	**39.35**
IND6	I only download software or programme from trusted sources.	4	**2.58**	5	**3.23**	36	**23.23**	71	**45.81**	39	**25.16**
IND7	I do not share my password to my colleage and family.	2	**1.29**	21	**13.55**	25	**16.13**	38	**24.52**	66	**42.58**
IND8	I do not leave my computer or laptop unattended.	9	**5.81**	9	**5.81**	25	**16.13**	35	**22.58**	75	**48.39**
IND9	I have skills to protect my computer and private data.	18	**11.61**	13	**8.39**	79	**50.97**	30	**19.35**	15	**9.68**
IND10	I feel secure when I can access my cloud data storage at any place and anytime.	3	**1.94**	20	**12.90**	40	**25.81**	29	**18.71**	58	**37.42**
	Average		**3.74**		**10.00**		**26.32**		**32.26**		**27.68**
		13.74		26.32				59.94			

Table 2 above shows individual factor frequency with most of the respondent responded “Agree” with the percentage average of 59.94% for IND1 until IND10. Around 26.32% respondents responded “Natural” for IND1 until IND10. The least average for IND1 and IND10 is 13.74%. Table 3 shows the respondent’s response on the organization factor frequency. The highest average responses in this section are on scale 1 and 2 “Disagree”. The percentage average for ORG1 to ORG 11 is 50.26%. Only 28.21% of the respondents responded “Agree” on organizational factor and 21.52% responded “Natural”. Table 4 shows the respondent’s response on information security awareness factor. The highest average responses in this section are on scale 4 and 5 “Agree”. The percentage average for ISA1 to ISA8 is 46.45%. Only 23.43% responded “Natural” on Information Security Awareness factor and 30.13% responded “Disagree”.

Table 3
Organization factor frequency

B	ORGANIZATION FACTOR	1	%	2	%	3	%	4	%	5	%
ORG1	The organization have a information security policy and procedures to be follow.	63	**40.65**	86	**55.48**	6	**3.87**	0	**0.00**	0	**0.00**
ORG2	I am aware of policy and procedure which are implemented in my organisation.	12	**7.74**	143	**92.26**	0	**0.00**	0	**0.00**	0	**0.00**
ORG3	I know content of the policy and procedures apply in the organization.	64	**41.29**	87	**56.13**	4	**2.58**	0	**0.00**	0	**0.00**
ORG4	Information security policy and procedures affect my behavior.	29	**18.71**	94	**60.65**	19	**12.26**	4	**2.58**	9	**5.81**
ORG5	My daily activity follow the organization information security policy and procedures	71	**45.81**	58	**37.42**	25	**16.13**	1	**0.65**	0	**0.00**
ORG6	My colleagues' information security behavior influences my behavior.	1	**0.65**	7	**4.52**	101	**65.16**	40	**25.81**	6	**3.87**
ORG7	Information security culture in my organisation influences my behavior	1	**0.65**	11	**7.10**	77	**49.68**	57	**36.77**	9	**5.81**
ORG8	My superior, peer or lecturer influence my security behavior.	10	**6.45**	51	**32.90**	37	**23.87**	49	**31.61**	8	**5.16**
ORG9	The organization provide secure network to students and staffs	24	**15.48**	21	**13.55**	35	**22.58**	62	**40.00**	13	**8.39**
ORG10	The students and employee who break information security rules will be discipline by the organisation.	1	**0.65**	17	**10.97**	25	**16.13**	97	**62.58**	15	**9.68**
ORG11	I am always doing the best practice behavior when dealing with the Internet.	1	**0.65**	5	**3.23**	38	**24.52**	95	**61.29**	16	**10.32**
	Average		**16.25**		**34.02**		**21.52**	10	**23.75**		**4.46**
		50.26			**21.52**			**28.21**			

Table 4
Information Security Awareness factor frequency

C	INFORMATION SECURITY AWARENESS	1	%	2	%	3	%	4	%	5	%
ISA1	Students and staff have been exposed to security awareness campaign by the organisation.	70	**45.16**	74	**47.74**	10	**6.45**	1	**0.65**	0	**0.00**
ISA2	Security awareness campaign influence my behavior.	10	**6.45**	93	**60.00**	28	**18.06**	19	**12.26**	5	**3.23**
ISA3	My experience increases my ability to have a safe behavior in term of information security.	11	**7.10**	30	**19.35**	99	**63.87**	15	**9.68**	0	**0.00**
ISA4	My experience helps me to recognize and assess information security threat.	6	**3.87**	0	**0.00**	29	**18.71**	109	**70.32**	11	**7.10**
ISA5	My experience helps me to perform best practice and avoid any misbehavior activities in information security	1	**0.65**	6	**3.87**	35	**22.58**	94	**60.65**	19	**12.26**
ISA6	I accept any kind of advice from others (peer, family, lecturer, Head of department). It is important to me if they suggest to me to use anti virus or anti-spyware in my computer.	9	**5.81**	0	**0.00**	25	**16.13**	65	**41.94**	56	**36.13**
ISA7	I accept any advice from other sources (College, Internet) to regularly update my password	1	**0.65**	10	**6.45**	29	**18.71**	86	**55.48**	29	**18.71**
ISA8	If others (peer, lecturer, Head of Department, IT Office) suggest to me to do backup, or not open appropriate web site, I would accept it.	1	**0.65**	5	**3.23**	23	**14.84**	53	**34.19**	73	**47.10**
	Average		**8.79**		**17.58**		**22.42**		**35.65**		**15.56**
		26.37			22.42			51.21			
	Total Average (%)	**30.13**			**23.42**			**46.45**			

Figure 1 below shows a low positive correlation and coefficient between X (Information Security Awareness) and Y (Individual) where r value is 0.110. The relationship between variable X and Y shows distant from being a perfect association. The graph shows us the small range of r value (0.110) supported by [24].

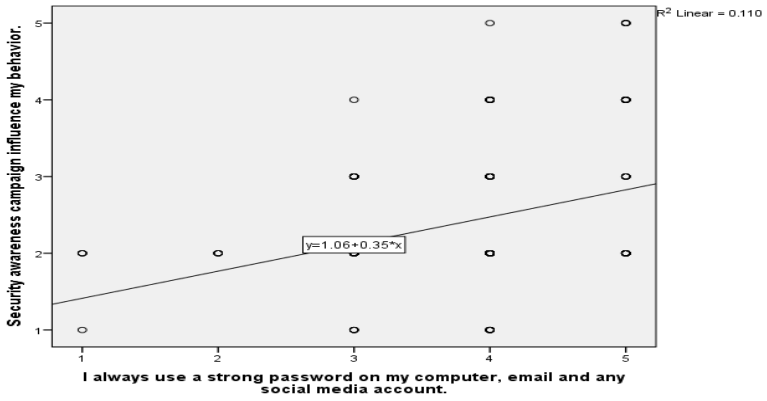


Fig. 1. A scatter diagram showing the relationship between variables

The relation of the individual factor, organization factor and information security awareness toward the awareness of security breach are positively correlated. Meanwhile, the degree of strength of the association is moderate (0.3< | r | < 0.5). Therefore, hypothesis null will be rejected. H_0: There is no relationship between independent variables and dependent variables H_1: to show a positive relationship between independent variables and dependent variables. Besides that, multiple linear regression is used in this study to investigate the relationship between independent variables (individual, organization and information security awareness) and dependent variables (the awareness of security breach) among IT users in KPTMBP. The stepwise model was adapted in this research study. Multiple regression is used because of various dependent variables exist ([25,26]). The regression will be conducted based on the predictor of the awareness of security breach.

Table 5
Summary of Multiple Regression Analysis

Regression Test	F value	Std. Error	R^2 (adj.)	Sig. (P Value)	Hypothesis Result
Individual	38.567	0.535	0.549	0.000	Supported
Organization	10.967	1.059	0.244	0.037	Supported
Information Security Awareness	13.502	0.673	0.448	0.00	Supported

Three multiple regression models were deployed. Individual factors tested were toward information security awareness and organization factor toward information security awareness. Individual factor regression shows the result of R^2 of 0.564, where it is statistically significant ($F(5,149) = 38.567$, $p < .005$) = 0.29. This indicates that individual knowledge in password management predicted nearly 54.9% of the difference on information handling, information security awareness experience, information security awareness campaign, and mobile computing. Next regression involves organization factor toward information security awareness. The R^2 organization regression value is 0.244, where it is statistically significant ($F(5,149) = 10.967$, $p < .005$). The outcome of this regression indicates that almost 24.4% of the variance in organizational effort to provide secure network was related towards information on security threat, information security experience, security awareness campaign, information handling and mobile computing. The next regression of Information security awareness indicates the adjusted R^2 is 0.448 where it is statistically significant $F(10,144) = 13.502$, $p < .005$). The outcome of this regression indicates that almost 44.8% of the variance in information security awareness was related towards organization factor, information security awareness and password management. Thus, the outcome from this regression analysis toward the awareness of information security breach was supported by the hypothesis of the

existence of a relationship between independent variables and dependent variables of the awareness of information security breach.

5. Discussion, future work, and limitation

5.1 Discussion

The knowledge towards human error, attitude toward policy and procedure and user behavior in information security awareness shows the relationship toward the awareness of security breach. The result is supported by previous researchers [5] who conducted research in determining employee awareness using the human aspect of information security questionnaire; the result showed knowledge toward policy and procedure is associated with attitude toward policy and procedure (R2 = 0.659**) and both are related to self-reported behavior (R2 = 0.777**).

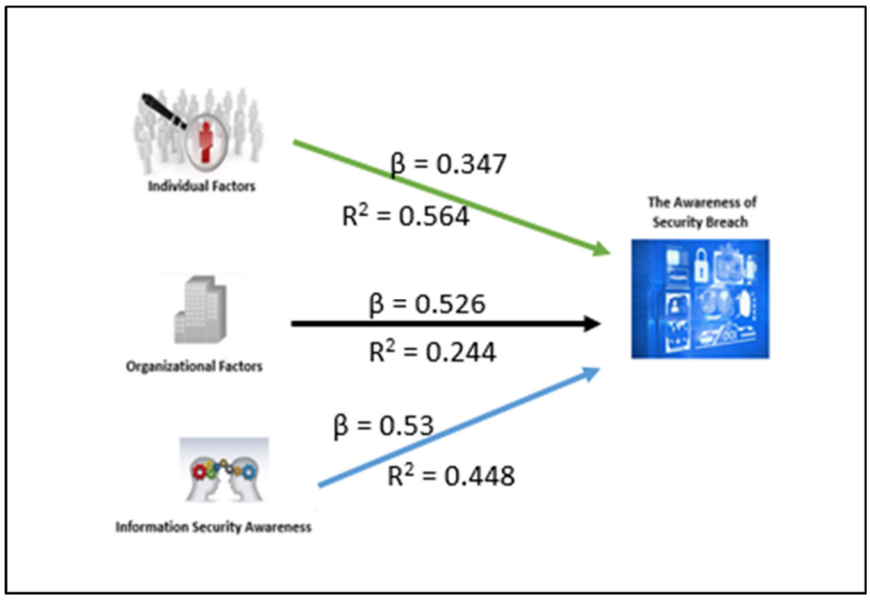


Fig. 2. The relationship between individual factors, organizational factor and information security awareness toward the awareness of information security breach.

The results shown in Fig. 2 specifies that individual factor, organizational factor and information security awareness shows a positive moderate relationship regarding the awareness of information security breach. However, the Beta (β) values stated in Fig. 2 indicates that information security awareness (β = 0.53) and organizational factors (β = 0.526), shows a strong relationship toward the organizational awareness of information security breach rather than individual (β = 0.347). Therefore, the derived models from the multiple linear regression models are as follows:

The Awareness of Information Security Breach$_1$ = 0.347(IND6) +0.347(IND2) + 0.308(ISA3) + 0.166 (ISA2) – 0.089(ORG9) +0.057(C)

The Awareness of Information Security Breach$_2$ = 0.526(IND2) +0.295(ISA3) – 0.190(ISA2) - 0.272 (IND10) +0.228(IND5) +0.765(C)

The Awareness of Information Security Breach$_3$	=	0.353(ISA3) - 0.888(ORG2) + 0.218(ORG3) + 0.219 (ORG7) +0.266 (ORG10) +0.272 (IND3) – 0.104 (ORG9) – 0.127 (ORG4) – 0.185 (ISA8) – 0.239 (ORG11) + 0.272 (IND3) + 2.077(C)

5.2 Future Work

Organization, mainly IT officers of KPTM Batu Pahat should be able to design and develop policies and procedures to improve organizational security awareness. Besides the organization's in-house IT personnel, the organization could also employ an independent consultant to design and develop Information Security Awareness Programme before implementation. Security awareness campaign, seminars and case study are the best approach to give exposure among IT users in Kolej Poly-Tech MARA Batu Pahat (KPTMBP). Furthermore, this research can also be conducted in different private and public colleges and universities that will cover a large range of population. Therefore, this research can serve as a pilot study for the other researchers conducting a survey in awareness of information security. Besides individual factor and organization factor, intervention factor can also be added to this study to measure and determine whether this factor have a significant effect on the awareness of information security breach by using a mediator to examine behavior of IT users in a given organization. Beside interviewing the IT officer, an interview with end user also should be conducted.

5.3 Limitation

One limitation faced by the researchers of this study is that human error is not tested in organizational factors and information security awareness factor, instead human error questions were focused solely on individual factors. Moreover, the sampling process in this study used only minimal sample sizes. The optimum sample size should come from at least 30% out of 1100 individuals in KPTM BP. However, this study only utilized responses from 155 respondents to describe the overall experience of IT users in Kolej PolyTech MARA Batu Pahat. The order of the questions may also have an impact on the user mindset regarding the questions asked. The questionnaires were constructed using positive wording. There were no negative questions in this questionnaire. These factors may have influenced the respondents when they were filling out the questionnaires.

6. Conclusion

As a conclusion, this study has provided an overview of the awareness of information security, literature review on various types of human error, independent and dependent variables of the awareness of information security breach. Besides that, this study has also proposed a framework model based on the literature survey by using an adapted model. The relationship between dependent and independent variables was also ascertained using the Bivariate Pearson Correlation and Coefficient. Then Multiple Regression models were used to find the relationship between independent and dependent variables. The outcome of this study shows all of the predictors or the independent variables have a statistical significant with the dependent variable.

References

[1] Mohamed, D. "Combating the Threats of Cybercrimes in Malaysia: The Efforts, the Cyberlaws and the Traditional Laws." *Computer Law & Security Review* 29, no. 1 (2013): 66–76.

[2] Tayouri, D. "ScienceDirect The Human Factor in the Social Media Security –combining Education and Technology

to Reduce Social Engineering Risks and Damages." *Procedia Manufacturing* 3, (2015): 1096–1100.
[3] Veiga, A., Martins, N. "Improving the Information Security Culture through Monitoring and Implementation Actions Illustrated through a Case Study." *Computers & Security* 49 (2015): 162–76.
[4] Zainol, Z., Nelson, S.P., Malami, A. "Internal human based threats and security controls in computerized banking systems: evidence from Malaysia." *Procedia-Social and Behavioral Sciences* 65 (2012): 199-204.
[5] Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., Jerram, C. "Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q)." *computers & security* 42 (2014): 165-176.
[6] Ahmed, M., Sharif, L., Kabir, M., Al-Maimani, M. "Human errors in information security." *International Journal* 1, no. 3 (2012): 82–87.
[7] Ifinedo, P. "Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition." *Information & Management* 51, no. 1 (2014): 69-79.
[8] Ahlan, A.R., Lubis, M., Lubis, A.R. "Information Security Awareness at the Knowledge-Based Institution: Its Antecedents and Measures." *Procedia Computer Science* 72 (2015): 361-373.
[9] Shaw, R.Sh., Chen, Ch.S., Harris, A.L., Huang, H-J. "The impact of information richness on information security awareness training effectiveness." *Computers & Education* 52, no. 1 (2009): 92-100.
[10] Said, A.R., Abdullah, H., Uli, J., Mohamed, Z.A. "Relationship between organizational characteristics and information security knowledge management implementation." *Procedia-Social and Behavioral Sciences* 123 (2014): 433-443.
[11] Montesdioca, G.P.Z., Maçada, A.C.G. "Measuring user satisfaction with information security practices." *Computers & Security* 48 (2015): 267-280.
[12] Thiab, A.S., Shibghatullah, A.S. "Hypervisor Security Issues in Cloud Computing: The Need to Mitigate the Risks." *Advanced Research in Computing and Applications* 1, no. 1 (2015): 1–5.
[13] Bhatti, F.N., Ahmad, R.B., Bhatti, H.M., Warip, M.N.M., Elias, S.J. "A Review and Survey of Vehicular Network' S Cybercrime and Security Approaches" *Advanced Research in Computing and Applications* 2, no. 1 (2016): 25–38.
[14] Reason, J. "Achieving a safe culture: theory and practice." *Work & Stress* 12, no. 3 (1998): 293-306.
[15] Al-Omari, A., El-Gayar, O., Deokar, A. "Security policy compliance: User acceptance perspective." In *System Science (HICSS), 2012 45th Hawaii International Conference on*, pp. 3317-3326. IEEE, 2012.
[16] Pahnila, S., Karjalainen, M., Siponen, M.T. "Information Security Behavior: Towards Multi-Stage Models." In *PACIS*, p. 102. 2013.
[17] Allam, S., Flowerday, S.V., Flowerday, E. "Smartphone information security awareness: A victim of operational pressures." *Computers & Security* 42 (2014): 56-65.
[18] Safa, N.S., Sookhak, M., Solms, R.V., Furnell, S., Abdul Ghani, N., Herawan, T. "Information security conscious care behaviour formation in organizations." *Computers & Security* 53 (2015): 65-78.
[19] Yen, D.C., Wu, Ch.-Sh., Cheng, F.-F., Huang, Y.-W. "Determinants of users' intention to adopt wireless technology: An empirical study by integrating TTF with TAM." *Computers in Human Behavior* 26, no. 5 (2010): 906-915.
[20] Weiss, Th., Loebbecke, C. "Online Gaming Adoption in Competitive Social Networks: Combining the Theory of Planned Behavior and Social Network Theory." *AMCIS 2008 Proceedings* (2008): 305.
[21] Kruger, H.A., Kearney, W.D. "A prototype for assessing information security awareness." *computers & security* 25, no. 4 (2006): 289-296.
[22] Jen, W., Lu, T., Liu, P.-T. "An integrated analysis of technology acceptance behaviour models: Comparison of three major models." *MIS Review* 151 (2009): 89-121.
[23] Da Veiga, A., Martins, N., Eloff, J.H. "Information security culture–validation of an assessment instrument." *Southern African Business Review* 11, no. 1 (2007): 147-166.
[24] Cohen, M.A. "Some new evidence on the seriousness of crime." *Criminology* 26, no. 2 (1988): 343-353.
[25] Huang, H.-M., Liaw, S.-S. "Exploring users' attitudes and intentions toward the web as a survey tool." *Computers in human behavior*21, no. 5 (2005): 729-743.
[26] Mathieu, J.E. "A causal model of organizational commitment in a military training environment." *Journal of Vocational Behavior* 32, no. 3 (1988): 321-335.