Journal of Engineering Technology Vol. 6: 1-5, 2018
ISSN 2231-8798

Towards The Impact of Social Engineering (SoE) Attacking Risk Factors in Higher Learning Institute

Shekh Abdullah-Al-Musa Ahmed [1], Nik Zulkarnaen Khidzir[2] & Tan Tse Guan[3]
[1] Faculty of Creative Technology and Heritage, University Malaysia Kelantan, Malaysia of Electronics Technology
[2]Global Entrepreneurship Research and Innovation Faculty of Creative Technology and Heritage, University Malaysia Kelantan, Malaysia
[3]Faculty of Creative Technology and Heritage, University Malaysia Kelantan, Malaysia

[1]Corresponding email: almusa.c17e002f@siswa.umk.edu.my

Abstract: In the Information security domain the theory of social engineering attacking risk factors is in Social Engineering (SoE)attacks that has an impact which would be disturbed the personal productivity of higher learning institute. The dependent variable which are threat, vulnerability, digital evidence awareness factors and one independent variable that is personal disturbance factors is used in this paper. Moreover, using as an indicator in determining disturbance of personal productivity in higher learning institute. Since multiple regression by Partial least square (PLS-SEM) is use to examined the collection of data by a questionnaire which is relevant with Social Engineering (SoE) attacking risks. And the resulting point out three dependent variables significantly influences on the independent variable of personal productivity in higher learning institute. As a matter of fact, this study concludes that the foremost influence factor on disturbance of personal productivity in higher learning institute towards the Social Engineering (SoE) attacking risk factors such as threat, vulnerability, digital evidence awareness factors. This study contributes to introductory study but vibrant understanding in stimulating the higher learning institute to become a worldwide institution.

Keywords: Digital evidence awareness factors, Social Engineering(SoE) attacking risks , Threat, Vulnerability.

1.0 INTRODUCTION

The higher learning institution is one of the special learning centers for any university as well as other expert area. All over the world every university has several higher learning institutions. Institution keep good communication with university by internet, file sharing and as well as knowledge sharing. The growing demand of higher learning institution is due to high quality education system as well as information and communication service. The increasing amount of learner in the institute also resulting the demand towards learner or students about the personal productivity inside the institution. This is the emerging for higher learning institution that should focus everywhere in the world. In recent time, the studies of higher learning institution are well conducted due to inter connected, database server with university and internet connection to determine to improve the personal productivity in learning but that can be disturbed or cause problem if there is any natural disaster such as any information security attacks such as Social Engineering (SoE) attacks may happened However, in this article focusing the Social Engineering (SoE) attacks that may stop the server database or unauthorized access of data in higher leaning institution and due to this attacks there would be an influence on personal productivity (Ringle et al.,2012).

Whereas the theory of Social Engineering (SoE) attacks in determining the disturbance of personal learning productivity who are studying the higher learning institute. However, the internet connection all over the institute may cause the vulnerability of the system. The Social Engineering (SoE) attacker always find out the open ports in the server. Hence the malicious person or Social Engineering (SoE) attacker try to implement the weak point of the institute, which is the Social Engineering(SoE) attacking threat factors in the institute. Whereas another factors are digital evidence awareness factors. The main motive of Social Engineering (SoE) attacker is to steal the digital evidence which would be caused the disturbance of

personal productivity in higher learning institute. The digital evidence or information in the higher learning institute server is the sensitive assets. So any loss of digital information assets is the Social Engineering(SoE) attacking risks. However, there is in sufficient literature study regarding the disturbance of personal productivity in higher learning institute. Thus, the theory of productivity in higher learning institute is capable in clarifying the disturbance of personal productivity if any information security attacks such as Social Engineering(SoE) attacks may happened in the institution Therefore any kind of Social Engineering (SoE) attacks that may have happened in higher learning institution and that would be caused the disturbance of the personal productivity of learner such as student in the learning institute (Sarstedt et al.,2014).

2.0 LITERATURE REVIEW

In this section, analyzing of theory of personal productivity in higher learning institute and literature related to hypothesis which would be development and discussed.

A. Theory of personal productivity learning

In this article, it is shown that four items which is related with personal productivity of higher learning and due to Social Engineering (SoE) attacks having the disturbance of personal productivity in the institute. The theory of disturbance of personal productivity is the dependent variable. The influence or the impact is not only disturbance of productivity it also showed the immoral impact in the institution. However, the productivity value makes a diverse influence in any specific social engineering attacks may happen in higher learning institution. Literature shows studies regarding the theory of personal productive learning has been applied in various studies in determining the stimulus in disturbance of personal productivity in the institution. Here in this article highlighted that there are three factors which influenced the personal productivity in learning towards the disturbance of personal productivity in higher learning institute.

B. SoE attacking Risk of Threat factors

Hence SoE attacking Risk Threat factors is shown when the Social Engineering (SoE) attacker utilize the vulnerability or weak factors or understand the weak point in the higher learning institute, however it might get effect on the information assets in the institute. Whereas in information security the SoE attacking threats shows the loss of institution assets or unauthorized access of data . Furthermore, it is emphasized that individual server, individual network or the entire networking in the higher learning institution. In the perspective of disturbance of personal productivity and towards the personal productivity in the institute. Threat factors are salience due to the live internet connection when students or learners decided to doing some creative or productive work. Thus, the following hypothesis is developing H1: Threat Factors that plays a significance role in disturbing the personal productive towards higher learning institute.

A. SoE attacking Risk of Vulnerability factors

The vulnerability concern is showing weakness control system inside the higher learning institute. Literature shows that vulnerability is a measurement of how effective or more precisely how in effective the control system inside the institute. If countermeasure is 100% effective against threats, with no weakness, then vulnerability would be zero. Though no control system in the institution is 100% perfect. This following hypothesis is developed H2: vulnerability concern is significant towards the disturbance of personal productivity in higher learning institute.

B. SoE attacking Risk of digital evidence awareness factors

Since social engineering is a term that basically used at first in political science area. Where its mean to influence particular attitude and social behavior in large scale. To produce desired characteristics in a target population by government, media or private groups. Whereas in information security the SoE attacking digital evidence awareness factors shows the loss of institution assets or unauthorized access of data. Furthermore, it is emphasized that lack of documentation of institutional service provider activities, individual network or the entire networking in the higher learning institution. In the perspective of disturbance of personal productivity and towards the personal productivity in the institute. digital evidence awareness factors are salience due to the live internet connection when students or learners decided to doing some creative or productive work. Thus, the following hypothesis is developing H3: digital evidence awareness factors that plays a significance role in disturbing the personal productive towards higher learning institute.

3.0 METHODOLOGY

In this section, the methodology of the research is discussed. Additionally, the research framework in introduced and data collection and data analysis to find out the impact of SoE attacks in higher learning institute.

A. Research framework

A research framework for this study is developed based on the theoretical background and literature review in this section, however, Figure 1 illustrates the research framework and the hypothesis for the SoE attacking risk factors. A questionnaire was distributed to a higher learning institute and getting the response (Hair et al., 2014). The questionnaire was adapted from inside the higher learning institute to asked to rate the questionnaire with each response being measured using 5 point Likert scale (1=very low, 2=low, 3=medium, 4=high, 5=Very high).

B. Sample characteristics

Total 168 questionnaires were distributed and 88 returns so, 53% response rate. The demographic of the respondent is shown in Table 1.

C. Result and Data Analysis

To test the hypothesis, a non-parametric structural equation modelling(SEM) by partial least square (PLS) analysis is done for higher learning institute. It is seen that PLS is a suitable approach to find out the impact value. When Social Engineering(SoE) attacks may happen into higher learning institution. And impact showing when this factor variable may effect learner or students and how much disturbance might feel when SoE attacks might happened (Aibinu et al., 2010).

D. Measurement Analysis

Kaiser-Meyer-Olkin (KMO) and Bartlett's test of sphericity is user to access the factor sample adequacy for analysis. The value of KMO must be greater or equal to 0.6. In this study, the KNO result is considered a good as it is achieved 0.863. While Barlett's test of sphericity is showing the high significant value ($p<0.001$) (Krombholz et al., 2015). Later, variable factor analysis is employed to test the discriminant validity of the item. In the Threat variable there are ten factors (Th1, Th2, Th3, Th4, Th5, Th5, Th6, Th7, Th8, Th9, Th10). For vulnerability possess ten factors (Vul1, Vul2, Vul3, Vul4, Vul5, Vul6, Vul8, Vul9, Vul10). And digital evidence awareness are ten factors(DE1,DE2,DE3,DE4,DE5,DE6,DE7,DE7,DE8,DE9 ,DE10).

And the variable disturbance of personal productivity possesses four factors (PP1, PP2, PP3, PP4). Questionnaire was designed according the factors name. When questionnaire was distributed among higher leaning institute and tried to find out the impact. However, in information security domain the methods of Social Engineering (SoE) attacks usually uses Trojan horse malware. So, how much disturbance would feel when learning would see to stop or disturbance of their work.

But from the factor analysis (Th2, Th8, Th9, Vul1, Vul3, DE1, DE5) has been removed due to the low factor loading (<0.6). Furthermore, the assessment of convergent validity has assessed the value of average variance extracted (AVE) of the variable such as threat, vulnerability and digital evidence awareness factors. The value of AVE must be above than 0.5. The result in Table 2 demonstrates that convergent validity is satisfied with the threshold value.

Additionally, to access the discriminant validity, the square root of AVE must be greater than inter-construct correlation (Lowry et al., 2014). The result of discriminant validity is shown in Table 3 which is diagonal value represents the square root of AVE. As a final composite reliability (CR) and Cronbach Alpha coefficient are used to assess reliability, as shown in Table 4, the CR value of 0.8, and the Cronbach alpha is greater than 0.7. This result shows that the reliability of construct is reliable.

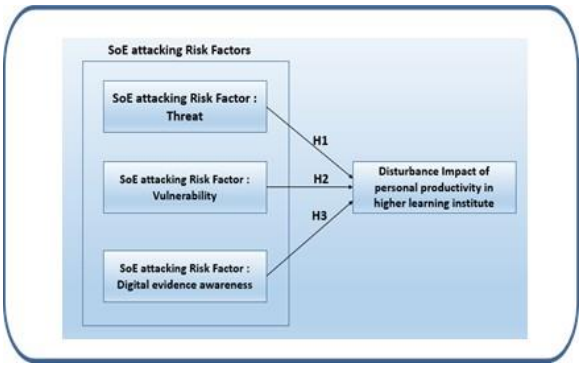

Figure 1: Research framework

4.0 PATH MODEL ASSESSMENT

It is valid to access the multi collinearity issue in the model. As shown in Table 5, VIF value between construct is less than the threshold value (5.0). The value shown in Table 5 demonstrates that the multi collinearity issue is not happening in the model.

The result of path assessment is shown in Table 5. The bootstrap technique was done to test the significance of the model. A sub-sample of 500 is used with 0.05 significance level. The value for path coefficient result as shown in Figure 2 and Table 4 indicates that the relationship (DE1, DE2, DE3, DE4). The study express that a positive and direct impact on countermeasure to disturbance of personal productivity towards the vulnerability in the higher learning institute ($P<0.001$) .

This result indicates that threat value of the system plays a significance role in determining the disturbance of personal productivity regarding higher learning institution (Lowry et al.,2014).

Journal of Engineering Technology Vol. 6: 1-5, 2018
ISSN 2231-8798

Additionally, in the path model all variable factors are connected to disturbance of personal productivity. This shows that the impact effect, when Social Engineering(SoE) attacks happened in the higher learning institute. And after the survey in the institution it is shown awareness of SE attacking risk (Mukkamala et al.,2005).

Lastly, there is a direct influence between the variable factors towards the disturbance of personal productivity. Since the impact is 0.584, which is showing the moderate effect happening in the case any SE attacking may happen in higher learning institute. As a final point the coefficient deamination R squared value for a dependent variable which is the disturbance of personal productivity is 58% where P<0.001. This endogenous construct manifests a high level of capturing variance which means that its well predicted by exogenous constructs.

Table 1: Demographic

		Frequency	%
Gender	Male	19	27.9
	Female	48	72.1
Age	21-30 Years	57	85.6
	31-40 years	9	12.9
	41-50 years	2	2.5
Education	Diploma	4	5.5
	Degree	15	21.9
	Postgraduate	61	75.6

Table 2: KMO and Barletts test of sphericity

KMO measure adequacy sampling		0.0862
Barlett's test of approximately. Chi squared		937.88
Sphericity	DF	171
	Sig	0.000

Table 3: Discriminate validity.

SoE attacking risk factors	Cronbach Alpha	CR	AVE
SoE attacking risk factor of threats	0.885	0.928	0.812
SoE attacking risk of vulnerabilities	0.723	0.843	0.663
SoE attacking risk of digital evidence awareness	0.810	0.922	0.707

Table 3: Discriminate validity

	Disturbance impact of personal productivity in higher learning institute	SoE attacking risk factor of threats	SoE attacking risk factor of vulnerabilities	SoE attacking risk of digital evidence awareness factors
Disturbance impact of personal productivity in higher learning institute	0.766	0.674		
SoE attacking risk factor of threats	0.663	0.532	0.724	
SoE attacking risk factor of vulnerabilities	0.875	0.661	0.687	
SoE attacking risk of digital evidence awareness factors	0.742	0.614	0.526	

5.0 DISCUSSION AND CONCLUSION

Theory of personal productivity has been employees in this study to investigate the disturbance of personal productivity when Social Engineering(SoE) attacking risks such as vulnerabilities, threats and digital evidence awareness factor of information security attacks happened in the higher learning Institution. For analysis and verification, multiple linear regression analysis was used. Threat factors value, vulnerability factors value and digital evidence awareness factors are the independent variable which is affected by dependent variable that is the disturbance of personal productivity regarding in higher learning institution is the dependent variable. The impact of Social Engineering(SoE) attacks has a significant impression towards personal productivity regarding in the higher learning Institution. It is happening because digital evidence awareness factors are the variable, that is showing how the institution takes SoE attacking risk. From this investigation can see that the impact is moderate if this kind of attacks happened.

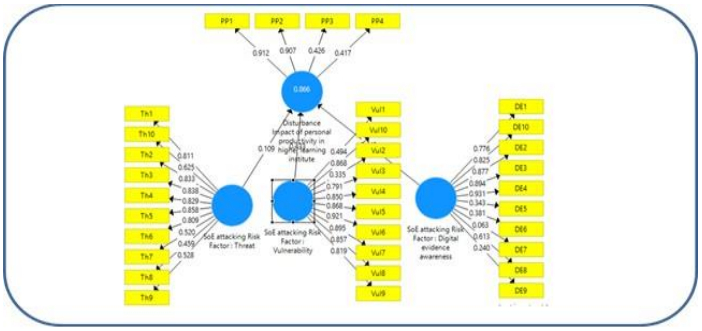

Figure 2 : Showing the path Model

Hence the institution is aware and as well as learner is aware about this kind of information security attacks such as Social Engineering (SoE) attacks. It is evidence that hundred present protection is impossible. However Trojan horse is a special type of malware that relies is large part on Social Engineering (SoE) attacks. Where this type of malware stops the firewalls and anti-virus software. In that case machine is controlled by malicious person. They are interested in gaining information which causes catastrophic impact in the institution. And it causes the disturbance of personal productivity. This is due to the SoE attacks in the institution.

Threat factors value has a significant impact on disturbance of personal productivity. This is due to information and communication development in the institution within the university. There is an opportunity for the institution to enhance the information security protection against Social Engineering (SoE) attacks, such a standardization of the guidelines and polices across the university. This study also suggests the university and related institution and increasing the awareness among the learners against this kind of attacks in the higher learning intuition.

REFERENCES

[1] Ringle CM, Sarstedt M, Straub D (2012) A critical look at the use of PLS-SEM in MIS Quarterly. MIS Quarterly 36: 3-15.

[2] Hair JF, Hult GTM, Ringle C, Sarstedt M (2014) A primer on partial least squares structural equation modelling (PLS-SEM). SAGE.

[3] Wong KKK (2013) Partial least squares structural equation modelling (PLS- SEM) techniques using Smart PLS. Marketing Bulletin 24: 1-32.

[4] Kock N (2015) A note on how to conduct a factor-based PLS-SEM analysis. International Journal of e-Collaboration 11: 9.

[5] Hair JF, Sarstedt M, Hopkin L , Kuppelwieser VG (2014) Partial least squares structural equation modelling (PLS-SEM) An emerging tool in business research. Emerald Group Publishing Limited 26:106-121.

[6] Aibinu AA, Al-Lawati AM (2010) Using PLS-SEM technique to model construction organizations willingness to participate in e-bidding. Automation in Construction 19: 714-724.

[7] Sarstedt M, Ringle CM, Smith D, Ream R , Hair JF (2014) Partial least squares structural equation modelling (PLS-SEM): A useful tool for family business researchers. Journal of Family Business Strategy 5: 105-115.

[8] Sarstedt M, Henseler J, Ringle CM (2011) Multigroup analysis in partial least squares (PLS) path modelling: Alternative methods and empirical results. Measurement and Research Methods in International Marketing Advances in International Marketing 22: 195-218.

[9] Lowry PB, Gaskin J (2014) Partial least squares (PLS) structural equation modelling (SEM) for building and testing behavioral causal theory: When to choose it and how to use it. IEEE Transactions On Professional Communication 57: 123-146.

[10] Kock N (2015) One-tailed or two-tailed P values in PLS-SEM? International Journal of e-Collaboration 11: 1-7.

[11] Krombholz K, Hobel H, Huber M, Weippl E (2015) Advanced social engineering attacks. Journal of Information Security and Applications.

[12] Huber M, Kowalski S, Nohlberg M , Simon T (2009) Towards automating social engineering using social networking sites.

[13] Krombholz K, Hobel H, Huber M, Weippl E (2013) Social engineering attacks on the knowledge worker. International Conference on Security of Information and Networks.

[14] Nohlberg M (2008) Securing information assets: understanding, measuring and protecting against social engineering attacks, p:97.

[15] NY Conteh, PJ Schmick (2016) Cybersecurity: risks, vulnerabilities and countermeasures to prevent social engineering attacks. International Journal of Advanced Computer Research 6:2277-7970.

[16] Nelms T, Perdisci R, Antonakakis M ,Ahamad M (2016) Towards Measuring and Mitigating Social Engineering Software Download Attacks. USENIX Security Symposium, pp: 773-789.

[17] Mukkamala S, Sung AH, Abraham A (2005) Intrusion detection using an ensemble of intelligent paradigms. Elsevier 28: 167-182.

[18] Anderson RJ (2010) Security engineering: a guide to building dependable distributed systems. Wiley Publishing pp:1040.evolutionary Computing, Evolutionary Computing, Game Artificial Intelligence and Multiobjective Optimization.