Journal of
Applied & Computational Mathematics

Musa, Zulkarnaen and Tan ,J Appl Computat Math 2018, 7:4
DOI: 10.4172/2168-9679.1000422

Research Article Open Access

An Investigation of AI enabled SoE Attacking Impact in Higher Learning Institute: Structural Equation Modeling (SEM) Approach

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*
[2]*Global Entrepreneurship Research and Innovation, University Malaysia Kelantan, Kelantan, Malaysia*
[3]*Faculty of Creative Technology and Heritage, University Malaysia Kelantan, Malaysia*

Abstract

Theory of artificial enabled social engineering attacking risk factors are employed in this study to determine the impact that disturbed the personal productivity of higher learning institute of the user towards the AI enable SoE attacking. Five independent variable which are threat, vulnerability, valuation, countermeasure and personal disturbance factors using in this paper. Moreover using as an indicator in determining disturbance of personal productivity in an higher learning institute. Since multiple regression by using Structural Equation Modelling –Partial Least Square (SEM-PLS) is used to examine the collection of data by a questionnaire which is relevant with AI enable SE attacking risk. And the resulting point out three independent variable significantly influences the 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 AI enables SoE attacking risk factors such as threat, vulnerability, valuation and countermeasure. This study contributes to introductory study but vibrant understanding in stimulating the higher learning institute to become a worldwide institution.

Keywords: Social engineering (SoE); Threat; Valuation; Vulnerability countermeasure; Partial least square (PLS); Structural equation modelling

Introduction

Higher learning institution is one of the special learning centers for any university as well as other expert area [1]. 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 [2]. The growing demand of higher learning institution is due to high quality education system as well as ICT service [3]. The increasing amount of learner in the institute also resulting the demand towards learner or students personal productivity inside the institution [4]. 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 may happen [5]. However, in this article focusing the artificial enable social engineering attack that may stop the server database or unauthorized access of data in higher leaning institution [6]. Whereas another study employed theory of impact of social engineering attacks in determining the disturbance of personal learning productivity [7]. Then the theory of internet connection all time determine that any kind of threat may come from any parts of world. The theory of malicious person activity determine how much protection measurement taken by the higher learning institute and that might indicate the countermeasure of the institute [8]. Whereas the theory of institution assets determine the valuation [9]. And the theories of weakness of the institution determine the countermeasure score of the institution. However, there is in sufficient literature study regarding the disturbance of personal productivity in higher learning institute [10]. Thus, the theory of productivity in higher learning institute is capable in clarifying the disturbance of personal productivity if any artificial enable social engineering may happen in the institution and assist the institute, researcher and government bodies in order to regulate and making the planning to prevent of any kind of AI enable SoE attacks that may happen in higher learning institution and that will be disturb the personal productivity of learner [11].

Literature Review

In this section, an analysis of theory due to personal productivity in higher learning institute and literature related to hypothesis development are discussed [12].

Theory of personal productivity learning

It is emphasize that four properties are manifest to the theory of personal productivity learning to the theory of disturbance of personal productivity is a function of multiple production learning and the personal productivity value makes a diverse influence in any specific artificial enables social engineering attack may happen in higher learning institution [13]. 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 four variable which influenced the personal productivity in learning towards the disturbance of personal productivity in higher learning institute [14].

Threat factors

Threat factors is defined as that it might get effect on the assets in the institute. However in information technology threats shows the loss of institution assets or unauthorized access of data [15]. Furthermore,

***Corresponding author:** Shekh Abdullah-Al-Musa Ahmed, Faculty of Creative Technology and Heritage, University Malaysia Kelantan, Malaysia, Tel: +6 01156887375 ; E-mail: almusa.c17e002f@siswa.umk.edu.my

Received October 12, 2018; **Accepted** October 25, 2018; **Published** October 31, 2018

Citation: Musa, Zulkarnaen (2018) An Investigation of AI enabled SoE Attacking Impact in Higher Learning Institute: Structural Equation Modeling (SEM) Approach. J Appl Computat Math 7: 422. doi: 10.4172/2168-9679.1000422

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 [16]. Threat factors are salience due to the live internet connection when students or learners decided to doing some creative or productive work [17]. Thus, the following hypothesis is develop H1: Threat Factors that plays a significance role in determining personal productive disturbance towards higher learning institute [18].

Countermeasure factors

Countermeasure factors are specific value that put in place to mitigate threats. For example in the higher learning institute could put firewalls in place to stop unauthorized access to server and data within the institute environment. But in the case of artificial enable social engineering attack malicious person sends Trojan malware through open access ports, which is result to stop the firewall and antivirus software in the system [5]. From the literature, the following hypothesis is aroused H2: Countermeasure factors that would impact towards disturbance of personal productivity in higher learning institute.

Valuation factors

Valuation factors are specific estimated value to the institution of the assets that a risk sometimes referred to as the valuation risk. For example, it could be simple as a single server that contains in the institute website while learners or students might not concerned if an external party accesses the data [6]. After all institution website makes the data available to personal productivity. H3: valuation concern is significant towards disturbance of personal productivity in higher learning institute.

Vulnerability factors

The vulnerability concern is showing weakness control system inside the higher learning institute [7]. Literature shows that vulnerability is a measurement of how effective or more precisely how in effective the control system inside the institute. If countermeasure are 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 H4: vulnerability concern is significant towards the disturbance of personal productivity in higher learning institute.

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 AI enable SoE attack in higher learning institute [8].

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 risk factors of artificial enable social engineering attacks in this study [9]. A questionnaire was distributed to a higher learning institute and getting the response. 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).

Sample characteristics

Total 167 questionnaire were distributed and 87 returns so, 52% response rate. The demographic of the respondent is shown in Table 1.

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 [10]. When artificial enable social engineering attack 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 AI enable SE attack might happen.

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 ($p<0.001$). 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).

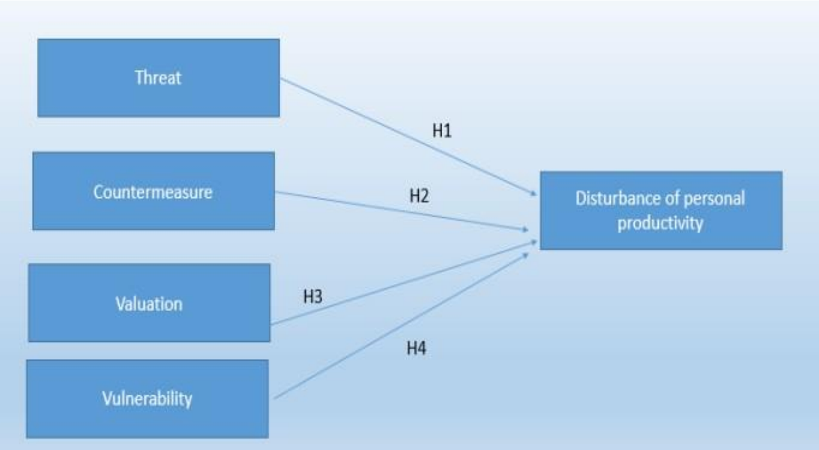

Figure 1: Research framework.

For countermeasure variable there are ten factors (Count 1, Count 2, Count 3, Count 4, Count 5, Count 6, Count 7, Count 8, Count 9, Count 10). For valuation variable there is only one Factor (Val1). And the variable disturbance of personal productivity possess four factors (PP1, PP2, PP3, PP4). Questionnaire was designed according the factor name. It is happened because of the respondent. When questionnaire was distributed among higher leaning institute and tried to find out the impact. When artificial enable social engineering such as 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, Count1, Count5) 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, countermeasure and valuation. 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 [11], to access the discriminant validity, the square root of AVE must be greater than inter-construct correlation. 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.

Path Model Assessment

It is valid to access the multicollinearity 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 multicollinearity 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 (PP1, PP2, PP3, PP4). 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) [12]. This result indicates that threat value of the system plays a significance role in determining the disturbance of personal productivity regarding higher learning institution.

		Frequency	%
Gender	Male	18	26.9
	Female	49	73.1
Age	21-30 years	58	86.6
	31-40 years	8	11.9
	41-50 years	1	1.5
Education	Diploma	3	4.5
	Degree	14	20.9
	Postgraduate	60	74.6

Table 1: Demographic.

KMO measure adequacy of sampling		0.863
Barlett's test of approximately. chi squared		938.86
Sphericity	**DF**	171
	Sig	0.000

Table 2: KMO and Barletts test of sphericity.

Variable factors	Cronbach Alpha	CR	AVE
Threat	0.886	0.929	0.813
Vulnerability	0.724	0.844	0.664
Countermeasure	0.811	0.876	0.64
Valuation	0.712	0.81	0.621
Disturbance of personal productivity	0.896	0.923	0.708

Table 3: Discriminate validity**.**

	Count measure	Disturbance of Personal Productivity	Threat	Valuation	Vulnerability
Count measure	0.658				
Disturbance of personal productivity	0.76	0.674			
Threat	0.664	0.534	0.725		
Valuation	0.876	0.662	0.688	0.791	
Vulnerability	0.741	0.615	0.527	0.822	1

Table 4: Discriminate validity.

	Disturbance of personal productivity
Count measure	4.484
Threat	1.982
Valuation	6.673
Vulnerability	3.142

Table 5: VIF value.

Additionally in the path model all variable factors are connected to disturbance of personal productivity. This shows that the impact effect, when artificial enable social engineering attacks happened in the higher learning institute. And after the survey in the institution it is shown awareness of AI enable SE attacking risk [13].

Lastly, there is a direct influence between the variable factors towards the disturbance of personal productivity [14]. Since the impact is 0.585, which is showing the moderate effect happening in the case any AI enable 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.

Discussion and Conclusion

Theory of personal productivity has been employees in this study to investigate the disturbance of personal productivity when artificial enable social engineering attacking enable social engineering attacking happen in the higher learning Institution. For analysis and verification, multiple linear regression analysis was used. Threat value, vulnerability value, countermeasure value and valuation are the independent variable while disturbance of personal productivity regarding in higher learning institution is the dependent variable. The countermeasure in the institution for AI enable social engineering attack has a significant impact towards personal productivity regarding in the higher learning Institution [15]. It is happens because countermeasure is the variable, that is Showing how much and how the institution takes protection against AI enable SE attacking risk. From this investigation can see that the impact is moderate if this kind of attacks happened. Hence the institution is aware and as well as learner is aware about this kind of attack. It is evidence that hundred present protection is impossible [16]. However Trojan horse is a special type of malware that relies is large part on artificial enable social engineering 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

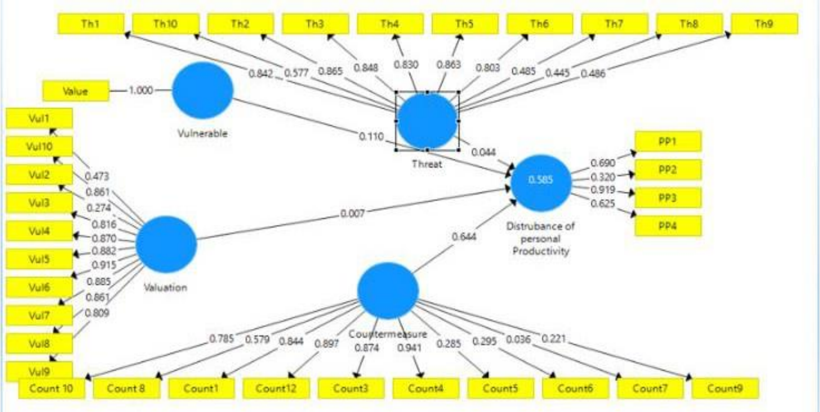

Figure 2: The path model.

is due to the AI enable SE attacks in the institution [17,18]. Threat 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 artificial enable social engineering 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.

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.

8. 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.
9. Kock N (2015) One-tailed or two-tailed P values in PLS-SEM? International Journal of e-Collaboration 11: 1-7.
10. Krombholz K, Hobel H, Huber M, Weippl E (2015) Advanced social engineering attacks. Journal of Information Security and Applications.
11. Huber M, Kowalski S, Nohlberg M , Simon T (2009) Towards automating social engineering using social networking sites.
12. Krombholz K, Hobel H, Huber M, Weippl E (2013) Social engineering attacks on the knowledge worker. International Conference on Security of Information and Networks
13. Nohlberg M (2008) Securing information assets: understanding, measuring and protecting against social engineering attacks, p: 97.
14. NY Conteh, PJ Schmick (2016) Cybersecurity: risks, vulnerabilities and countermeasures to prevent social engineering attacks. International Journal of Advanced Computer Research 6:2277-7970.
15. Nelms T, Perdisci R, Antonakakis M ,Ahamad M (2016) Towards Measuring and Mitigating Social Engineering Software Download Attacks. USENIX Security Symposium, pp: 773-789
16. Mukkamala S, Sung AH, Abraham A (2005) Intrusion detection using an ensemble of intelligent paradigms. Elsevier 28: 167-182.
17. Anderson RJ (2010) Security engineering: a guide to building dependable distributed systems. Wiley Publishing pp:1040.