# Social Engineering (SoE) Attacks Towards Network Security in Higher Learning Institute: The Partial Least Squares Path Modeling Approach

**Nik Zulkarnaen Khidzir[1*] ,Shekh Abdullah-Al-Musa Ahmed[2], Tan Tse Guan[3] and Khairul Azhar Mat Daud [4]**

*Faculty of Creative Technology and Heritage,*
*University Malaysia Kelantan,*
*Malaysia*

**Abstract**

**The basic network security issues have changed very little over the past decade. Protecting the confidential institutional information , preventing unauthorized access defending the network against SoE attacks remain primary concerns of network security professional toady. Widespread remote access by the high number of increasing sophisticated SoE attacks is making network security significantly more challenging in the institute . Confidential information can reside in two states on a network . It can reside on institutional physical storage media , such as a hard drive or memory , or it can reside in transit across the physical network wire in the form of packets. These two information states present multiple opportunities for SoE attacks from users in higher leaning institute internal network , as well as those users on the internet. Given the dramatic rise in external security threats , couples with the rising cost of network intrusions. Institution are more pressured than ever to define and protect their network perimeter . There is no choice for the institute but to keep abreast of large number of security issues confronting in today's world.**

## Keywords

**Network security, Social Engineering, SoE attacking risk of threats, SoE attacking risk of vulnerabilities , conceptual framework.**

## INTRODUCTION

Network security has become very complex today for the prevention technique of SoE attacks in Higher Learning Institute . Network security is the fundamental defences to safeguard the collaborative in Higher learning institute . As the convergence of higher learning institute network gain pace ,security issues for the computer networks for the prevention technique of SoE attacks become a top concern in the institute (Manske, K .,2006).

Since SoE attacks and network security are the context of domain in information security . SoE attacks refers to psychological manipulation of people into performing action to gain confidential information . Whereas SoE is the methods of attacks in networking .Therefore it is necessary to maintain Network security . The complexity of ensuring a reliable network security is viewed as the single most critical barrier to the successful implementation of net-centric information system( Korchenko et al.,2010) .

Though it is evidence that number of methods of SoE attacks increasing . Typically types of SoE attacks consists of mobile based SoE attacks , computer based SoE attacks and human based SoE attacks and all are connected with networking . The activities SoE attacks on networking are also escalating. Thus , to counter the SoE attacking risks of threats , SoE attacking risks of vulnerabilities are increasing and network security is the first line of defence for the prevention technique of SoE attacks in higher learning institute . Peripheral defences play an important role and so there is a need to establish perimeter security for protecting the network (Duff, A. S.,2005) . Consider the following simple example , within a network , it is possible to spot Trojan horse in many ways . For example port scanning can be very effective.

So that they can be neutralized before the attack on network begins . This is especially important given the growing number of 'zero-day' SoE attacks , which launch before or soon after the announcement of SoE attacking risks of vulnerabilities . In higher

leaning institute are networked in many sense of the term , not only socially but digitally network as well , the Internet being the mother of all networks . It is unthinkable in today's paradigm to work without the Internet and Web based IS. The higher learning institution is one of the special learning centres 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 (D'Arcy et al.,2014). 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 institution also resulting the demand towards learner or student .

Whereas the theory of Social Engineering (SoE) attacks in the networking issues in the higher learning institute . However , the internet connection all over the institute may cause the vulnerability of the networking 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 networking point of the institute , which is the Social Engineering (SoE) attacker threats factors in the institute . Therefore any kind of Social Engineering (SoE) attacks that may have happened in higher learning institution , the effect would be personal productivity in the higher learning institute (Brotby, W. K. et al.,2013) .

## LITERATURE REVIEW

The digital world evolves , complexities and SoE attacks may happened from any parts of the world. In that case network security experts would have all the robust , seamless communication network connectivity in the institution. That would make the communication internetwork , composed of tactical radio nets , satellites , microwave , landline links etc. Whereas network expert called this seamless for two reasons – first , because that would be able to transmit some data network leaner in the institution , second because the technical difficulties of linking the separator network types would be hidden from most developers as well as users , that would be the vulnerable parts of network by SoE attackers .

There would be many higher learning institute that would be connected by single seamless network . Even wars would be fought digitally . Although every battlefield entity would have a network presence . This showed that net-centric information and communication technology would be a fundamental target for SoE attackers in the higher learning institute (Cheung, S. K. S.,2005).

Bandwidth limits would still be a problem through especially in the combative situation and mobile computing situation and mobile computing . However always increase the capacity of the fixed landline segments for the network to meet increasing demand in higher learning institution. This would not always be possible for satellite and especially technical radio communication. In short , in the higher learning institution everyone get some data , anywhere but not always all data everywhere , would want , anywhere . Whereas in this article focusing about SoE attacking risks of vulnerability and SoE attacking risk of threats , but they had all been network technological in nature . SoE attacks dealt with targeting technology and manipulation of human who were involving to use the technology in higher learning institute . Several terms that are used in information security domains . Such a hacker is called to a person who has strong interest in computers who enjoys learnings and experimenting with them (Kebande, V. R. et al., 2018) .

In the social engineering attacks hacker are usually very talented smart people who understand computer network better than other in higher learning institution . The term is often confused with cracker that defines someone who breaks into computer system in the higher learning institute . Whereas brute force hacking is a technique used in higher learning institution to find passwords or encryption keys . Brute force hacking involves trying every possible combination and letters , numbers etc , until the code is broken . However , cracker is someone who breaks into computer network system should not be confused with hackers . The term cracker is usually connected to criminals. Some of their crimes include vandalism , student ID theft and snooping in unauthorized areas . Another term cracking refers the act of breaking into computer network system . Cracking is a popular growing subject on the internet . Many sites are devoted to supplying crackers with programs that allow them to creak computers.

Some of these programs contains dictionaries for guessing passwords . Other are used to break into phone lines (called ' phreaking ' ) . These sites usually display warnings such as " These files are illegal" . In that case , in the higher learning institution , learner would not responsible for what they would do . However cracker tools are programs used to break into computer system in higher learning institute . Cracker tools are widely distributed on the internet. They include password crackers , Trojan Horse , virus , war dialers and worms . Whereas phreaking is the notorious art of breaking into phone

or other communication systems . Phreaking sites on the internet are popular among crackers and other criminals (Manske, K. ,2006).

However the concepts of network security in higher learning institute are related to the security of the networking and other related terms . Hence , Emission Security (Emsec) refers to preventing a system being attacked using compromising emanations , that is conducted or radiated Electromagnetic signals . There are many aspects of Emsec . Military and defense , which prevent the stray Radio Frequency (RF) emitted by network and other electronics equipment's , from being picked up by a person and used to reconstruct the data being processed , though this requires extremely complex technical skills in the person attempting it , it is not impossible . Apart from defense and military organizations , smart card industry , too , is concerned with power analysis , in which a computation being performed by a smart card such as a digital signature is observed by measuring the electric current drawn by central processing unit (cpu) of a computer and the measurement results are used to reconstruct the key . Although people often undermine the important of Emsec , it is not something to be ignored . Social Engineering (SoE) related activities are notorious and loss a huge amount of valuable research data . Communication Security and Emsec were adequate , in the earlier days , when message were by teletype .Eventually , networking came on the scene in a big way and most of the Information assets of the higher learning institution became easier to use and more and more learner in the higher learning institution got to access them with interactive sessions (Peltier, T. R.,2006) . Thus , information on the system became accessible to almost everybody in the higher learning institute as long as they had access to them . This is when the need for network security was realized in the higher learning institution .

In the early 1970's , various model were developed for security , most famous among them being the 'La Padula' model . These security model was based on the concepts of 'governance' and level of classification information , unclassified , confidential , secrets , top secrets information (Sumner, M.,2009).

## METHODOLOGY

In this section the methodology of the research article is discussed . Additionally , the conceptual research framework for Social Engineering (SoE) attacks towards network security in higher learning institute . Data were collected from the higher learning institute, analysis would be done and determined
network security could prevent SoE attacks in higher learning institute .

In that case the conceptual framework for this study is to developed based on the theoretical background and previous literature review in this section. However Figure 1 illustrate the conceptual research framework and hypothesis for the relationship of SoE attacks and network security with higher learning institute . A survey questionnaire were distributed in higher learning institution . The questionnaire were adopted from various previous literature review and asked to the admin officers and ICT officer in the institute regarding their prediction of network security for the prevention technique of SoE attacks or not . However , five Likert scale was used in the questionnaire (Algarni, Aet al., 2017) .

In the sample collection section , there were total 87 questionnaire were distributed in the higher learning institute and 39 returns , so 44% response rate . A Shapiro-Wilk's test ($p>0.05$) (Shapiro & Wilk , 1995 ; Razali & Wah , 2011) and a visual inspection of their histogram , normal Q . However Q plots and box plots showed that for the research article . In that case , SoE attacking risk of threats , SoE attacking risks of vulnerability , Network Security were approximately normally distributed for higher learning institute , with a skewness of 0.373 (Standard Error = 0.361) and a Kuttosis of 0.583(Standard Error = 0.716) (Algarni, A et al.,2017), 2004 ; NY Cont eh et al., 2016).

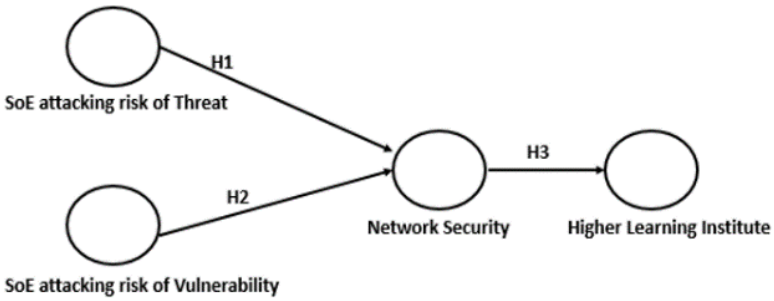


Figure 1 : Conceptual framework for SoE attacks towards network security in higher learning institute

## SPECIFY THE MEASUREMENT MODEL

Construct is a variable that not directly observed therefore , needed a measurement model for each construct . In this research article , there would be four construct (Thr , Vul , NS , H_I) measured by multiple items . All four construct to be indicator indicate a reflective measurement model . Each of these construct is measured by multiple indicators . For instance , the endogenous construct SoE attacking risks of Threats would be (Thr) is measured by (Thr1 , Thr2 , Thr3, Thr4, Thr5) . Then SoE
attacking risk of Vulnerability would be (Vul1, Vul2, Vul3, Vul4, Vul5, Vul6) . Whereas Network Security would be ( NS1, NS2, NS3, NS4 , NS5) . And the exogenous construct is the higher learning institute would be (H_I1,H_2,H_3,H_I4,H_I5) . In this case deploying the hypothesis for the path relationship which is :
H1: SoE attacking risk of Threats (Thr) will have a significance effect on Network Security (NS).
H2 : SoE attacking risk of Vulnerability (Vul) will have a significance effect on Network Security (NS).
H3: Network Security (NS) will have a significance effect on higher learning institute(H_I).

## REFLECTIVE MEASUREMENT ANALYSIS

The path model was prepared for the research article . That would demonstrate the variables relationship that have already described. However , in this research article the term construct would used to descried a variables that is called latent variable . Structural theories specifies how construct was related to each other in the structural model. Therefore in this research article it was needed a measurement model for analysis . As described before there were four construct (Thr, Vul, NS,H_I) measured by multiple items that would be displayed in the figure . All four construct have arrows pointing from the construct to the indicator to indicate a reflective measurement model.
Each of these construct were measured by multiple indicators . For instances the endogenous construct of SoE attacking risks of Vulnerability(Vul) were measured by vul1, vul2, vul3, vul4, vul5, vul6 and were other construct .
Result summary of reflective measurement for this research article :
Table 4.1 : Showing the reflective measurement model for this research model.

| Latent variable | Indicator | Internal consistency | | Convergent Validity | | Discriminant validity |
|---|---|---|---|---|---|---|
| | | Composite Reliability | Cronbach Alpha | Loading | AVE | HTMT confidence interval does not include 1 |
| | | 0.6-0.9 | 0.6-0.9 | >0.7 | >0.5 | |
| SoE attacking risks of Threat | Thr1 | 0.768 | 0.691 | 0.781 | 0.651 | Yes |
| | Thr2 | 0.282 | | | | |
| | Thr3 | 0.860 | | | | |
| | Thr4 | 0.582 | | | | |
| | Thr5 | 0.751 | | | | |
| SoE attacking risks of Vulnerability | Vul1 | 0.928 | 0.906 | 0.877 | 0.683 | Yes |
| | Vul2 | | | 0.686 | | |
| | Vul3 | | | 0.870 | | |
| | Vul4 | | | 0.842 | | |
| | Vul5 | | | 0.789 | | |
| | Vul6 | | | 0.877 | | |
| Network | NS1 | 0.769 | 0.790 | 0.860 | 0.683 | Yes |

| | | | | | | |
|---|---|---|---|---|---|---|
| Security | | | | | | |
| | NS2 | | | 0.393 | | |
| | NS3 | | | 0.692 | | |
| | NS4 | | | 0.842 | | |
| | NS5 | | | 0.711 | | |
| Higher learning institute | H_I1 | 0.716 | 0.645 | 0.760 | 0.544 | |
| | H_I2 | | | 0.714 | | |
| | H_I3 | | | 0.631 | | |
| | H_I4 | | | 0.714 | | |
| H_I5 | | | | 0.330 | | Yes |

## PATH COEFFICIENT FOR THE RESEARCH ARTICLE

As the matter of fact , the path coefficient for SoE attacks towards network security in higher learning institute had standardized value between -1 to +1 . When the path coefficient close +1 represented strong positive relationship and that would be statistically significance . However , sometimes path coefficient value has shown very low or close to 0 they were not significantly different from zero (Algarni, A et al., 2017) .

SoE attacking risk of threats( Thr) having path effect on Network Security (NS) in the higher learning institute would be (0.231) . SoE attacking risk of vulnerabilities (Vul) having path effect on Network Security (NS) in the higher learning institute would be (0.691). And Network Security (NS) having path effect on higher learning institute would be (0.410). Whether the path coefficient for SoE attacks towards network security in higher learning institute was significance , it should be evaluated for it standard error that could be attained from bootstrapping . The bootstrapping standard error that could be attained from bootstrapping .The bootstrapping standard error calculate the empirical t-value and p-value for all structural path coefficient . When an empirical t- values was larger than critical value . It would be concluded that the certain error probability or significance level. Generally used certain values for two tailed test was 1.96 (significance level = 5%). Instead of reporting t-value and p-value , it would be suggested also to report the bootstrap confidence interval , which showed whether a path coefficient was significantly different from zero . The bootstrap confidence interval was based on standard error derived from bootstrapping and specify the range into which the time population parameter would fall assuming a certain level of confidence (such as 95%) . If a confidence interval of this research model wouldn't include zero for an estimate path coefficient , the hypothesis that the path equal zero was rejected and concluded a significance effect (Taylor, R. G.,2015).

| | Original Sample (O) | Sample Mean (M) | Standard deviation(STDEV) | T-Statictics (O\|STDEV) | P-value |
|---|---|---|---|---|---|
| NS->H_I | 0.410 | 0.480 | 0.152 | 2.693 | 0.007 |
| Thr->NS | 0.231 | 0.392 | 0.210 | 2.132 | 0.005 |

| | | | | | |
|---|---|---|---|---|---|
| Vul->NS | 0.691 | 0.641 | 0.259 | 2.669 | 0.008 |

## NETWORK SECURITY IN HIGHER LEARNING INSTITUTE

As computer system evolved in higher leaning institute though networks and from the convenient survey it is evidence that it is network security would reduce the social engineering attacking risk .However another problem arose , that of lack network understanding for the protection of social engineering attacks . New security problems occurs when computer standards , emissions control etc come up in the domain of network security for higher learning institute in prevention social engineering attacks .

Basically , network security is used to control access to network resources and services in higher learning institute . There are three element of network security to the preventing technique of SoE attacks : cryptography , secure network protocol and application and access control mechanisms. However authenticity , integrity ,confidentiality , non repudiation are the basic properties that are expected from a network service provider . Hence the classification of network security are : trusted network , semi-trusted network and untrusted network. Whereas trusted network are the network inside the higher learning institute network security perimeter . These network are the ones that the institution need to protect from social engineering attacks. When a firewall server is set up , the network administrator must explicitly identify the type of networks that are attached to the institutional firewall server through network adapter cards (Singleton, T. W.,2008). After the initial configuration , the trusted networks include the firewall server and all network behind it . Hence there are networks dedicated to the institution , but not the physical control such as internet. These are also referred to as the demilitarized zone (DMZ) . Under the scenario of semi trusted networks, access is allowed to some database materials and electronic mail (e-mail). Semi-trusted networks may include domain name system(DNS) , proxy and modern server . However , they are not for confidential or proprietary information for the higher learning institute .

On the other hand untrusted network are the networks that are known to be outside of the institution security perimeter. Essentially , they are any network where the institution do not know the routing of messages such as internet or similar. They are untrusted because they are outside of the institution. There is no control over the administration or security policies for these sites . That are the private , shared networks from which the institution are trying to protect the network. However , institution may still need and want to communicate with these networks although they are untrusted. When setting up a firewall server in the higher learning institute for the protection of social engineering attacks , it is necessary to explicitly identify the untrusted networks from which that firewall can accept requests (Korchenkoet al.,2010). As said untrusted network are outside the institution security perimeter and are external to the firewall server.

## SoE ATTACKS ON NETWORKING

The social engineering attempts to attack in the higher learning institute to gain hold of the information resources on the network. The other way of classifying the SoE attacks on networking would be passive attacks mean that only the message transfer is monitored : unauthorized institutional release of a confidential message or using a message to determine the type of communications. Whereas active SoE attacks mean that the message is intercepted , modified or otherwise manipulated (Kebande et al.,2018). Masquerading is where SoE attacker pretends to be someone else , replay means that message are recorded and user to produce an authorized effect , message modification means that the message has been altered and SoE attacks prevent valid users from accessing the institution service.

## CONCLUSION

The partial least squares path modeling Approach it is evidence that in the higher learning institution network security is necessary for the prevention technique of SoE attacks . Network security is the process of intercepting and examining SoE attacker messages in order to deduce information patterns in communication . Hence network security can be performed even when the messages are encrypted and cannot be decrypted . In general , the greater the number of message observed in the institute , or even intercepted and stored, the more that can be inferred from the traffic . Network security such as traffic analysis can be performed in the context of higher learning institute and is a concern in network security against SoE attacks . When institutional network is connected to the internet , user are physically connecting with other institutional network , unknown networks all over the world. Although such

connection open the door to many useful applications and provide great opportunities for information sharing , most private networks contain some information that should not be shared with outside of the institutional users on the internet. Hence from the survey , it is evidence that network security is requied from SoE attacks , here network security professionals is protecting institutional confidential information and protecting the institutional network to maintain internal network system integrity under the SoE attacking risk of threats .

## COMPETING INTERESTS

Authors declares that they have no competing interests.


## FUNDING

Authors declare that there was no any funding received for conducting this study.

## ACKNOWLEDGEMENTS

We gratefully thankful to the University Malaysia Kelantan. We thank all the faculty member in UMK , and all the helping hands who support and help us in every step of our study.


## AUTHOR CONTRIBUTIONS

All the authors had equal contribution on this study. Task were separated to all authors according to their expertise on specific topic. Associate Prof Dr Nik Zulkarnaen Bin Khidzir generated the research topic for this study and reviewed relevant literatures. Dr Shekh Abdullah-Al-Musa Ahmed , Associate Prof Dr Tan Tse Guan and Associate Prof Dr.Khairul Azhar Mat Daud was the designer for the study. He designed methodology and analysis plan for the study and analyzed all the outcomes of the study and they also contributed on overall write up.

## REFERENCE


Abawajy, J. (2014). User preference of cyber security awareness delivery methods. Behavior & Information Technology, 33(3), 237-248.

Algarni, A., Xue, Y., & Chan, T. (2017). An empirical study on the susceptibility to social engineering in social networking sites: the case of Facebook. European Journal of Information Systems 26(6), 661-687.

Applegate, S.D. (2009). Social Engineering: Hacking the Wetware! Information Security Journal: A Global Perspective, 18(1), 40-46.

Brill,A., Pollit, M., & Whitcomb, C. M. (2006). The Evolution of Computer Forensic Best Practices: An Update on Programs and Publications. Journal of Digital Forensic Practice, 1(1), 3-11.

Brotby, W. K. & Hinson, G. (2013). PRAGMATIC Security Metrics: ApplyingMetametrics to Information Security .CRC Press.Buskirk, E.V. & Liu, V.T. (2006). Digital Evidence: Challenging the Presumption of Reliability. Journal of Digital Forensic Practice, 1(1), 19-26.

Cheung, S. K. S. (2005). Information Security Management for Higher Education Institutions. Intelligent Data analysis and its Applications, 1(2-3), 55-68.

Cremonini, M. & Nizovtsev, D., (2009). Risks and Benefits of Signaling Information System Characteristics to Strategic Attackers. Journal of Management Information Systems, 26(3), 241-274.

D'Arcy, J.,Herath, T.& Shoss, M.K. (2014). Understanding Employee Responses to Stressful Information Security Requirements: A Coping Perspective. Journal of Management Information Systems, 31(2), 285-318.

Duff, A. S. (2005) Social Engineering in the Information Age. An International Journal, 21(1), 67-71.

Gonzales, R., Llopis, J. & Gasco, J. (2013). Information technology outsourcing in financial services. The Service Industries Journal, 33(9-10), 902-924.Hinson, G. (2007). The State of IT Auditing in 2007. The EDP Audit, Control, and Security Newsletter, 36(1), 13-31.

Kebande, V. R. & Venter, H. S. (2018). Novel digital forensic readiness technique in the cloud environment. Australian Journal of Forensic Sciences, 50(5), 552-591.

Kim, E.B. (2013). Information Security Awareness Status of Business College: Undergraduate Students. Information Security Journal: A Global Perspective, 22(4), 171-179.

Korchenko, O., Vasiliu, Y. & Gnatyuk, S. (2010). Modern quantum technologies of information security against cyber-terrorist attacks. Aviation, 14(2), 58-69.

Manes, G. W. & Downing, E. (2010). What Security Professionals Need to Know About Digital Evidence. Information Security Journal: A Global Perspective, 19(3), 124-131.

Kock N . (2015). One-tailed or two-tailed P values in PLS-SEM? International Journal of e-Collaboration 11(2) 1-7.

Manske, K. (2006). An Introduction to Social Engineering. Information Systems Security, 9(5), 1-7.Maruf, A., Islam, M. R. & Ahamed, B. (2010). Emerging Cyber Threats in Bangladesh: In Quest of Effective Legal Remedies. Northern University Journal of Law, 1(4), 112-124.
NY Conteh, PJ Schmick .(2016). Cybersecurity: risks, vulnerabilities and countermeasures to prevent social engineering attacks. International Journal of Advanced Computer Research ,6(2), 77-89.
Peltier, T. R. (2006). Social Engineering: Concepts and Solutions. Information Systems Security, 15(5), 13-21.
Pieters, W. (2011). The (Social) Construction of Information Security. The Information Society, Volume 27(5), 326-335.
Posey, C., Roberts, T. L.& Lowry, P. B. (2015). The Impact of Organizational Commitment on Insiders' Motivation to Protect Organizational Information Assets. Journal of Management Information Systems, 32(4), 179-214.
Ringle CM, Sarstedt M, Straub D . (2012) . A critical look at the use of PLS-SE Min MIS Quarterly. MIS Quarterly 36(2),3-15.
Sakil, A. H. (2018). ICT, youth and urban governance in developing countries: Bangladesh perspective, International Journal of Adolescence and Youth, 23(4), 219-234.
Singleton, T. W. & Singleton, A. J.(2008). The Potential for a Synergistic Relationship Between Information Security and a Financial Audit. Information Security Journal: A Global Perspective, 17(2), 80-86.
Sumner, M. (2009). Information Security Threats: A Comparative Analysis of Impact, Probability, and Preparedness. Information Systems Management, 26(1), 2-12.
Taylor, R. G. (2015). Potential Problems with Information Security Risk Assessments. Information Security Journal: A Global Perspective, 24(4-6), 177-184.
Wiebke, A. (2009). Agents, Trojans and tags: The next generation of investigators. International Review of Law, Computers & Technology, 23(1-2), 99-108.