Journal of
Mass Communication & Journalism

Research Article Open Access

An Exploratory Factor Analysis of AI Enabled SE Attacking Risk in Higher Learning Institute

Khidzir NZ[1]* and Abdullah-Al-Musa Ahmed S[2]

[1]*Global Entrepreneurship Research and Innovation Centre/Centre of Computing and Informatics, University Malaysia Kelantan, Malaysia*
[2]*Faculty of Creative Technology and Heritage, University Malaysia Kelantan, Malaysia*

Abstract

Any kind of business organization or individual organization one word is very common that is information. Depending on the information and its communication medium ensure the effective of business. Whereas it is very much essential to understanding Artificial Intelligence (AI) Enabled Social Engineering (SE) attacks and its security risk management approach. Under such circumstance, information is exchanged from one country to another country for various purposes. In that case, artificial intelligence enabled social engineering attack must be considered in any kind of organization. Any kind of business venture is disturbed by this kind of attacks which will be failure the business operation, whilst enabling them to concentrate on their core business activities. Social engineering is one kind of criminal activities in the information security. It has proven to be very successful way for a criminal to get inside an organization. Once social engineering got password from an employee, then snooping around the sensitive data. However social engineering are the types of attacks inherent risk and any kind of organization should be aware of its potential risks. So, it could be identify and resolved quickly. The objective of this article, therefore, conducting an Exploratory Factor Analysis (EFA) in artificial intelligence enabled social engineering attacks on various organizations. Which consequently provide knowledge of the most relevant information security risk factor. For this article distributed 300 questionnaires in education sector for the study and 110 were returned. That means the response rate is 36%. In that case, the finding of the article shows that threat and vulnerability factors in artificial intelligence enabled social engineering attacks. So, for any organization these two factors are the most for information security risk.

Keywords: Artificial intelligence enabled social engineering; Threat; Vulnerability; Factor analysis; Path model; Information security

Introduction

Social engineering is a very basic level of attacks. Once the malicious person gets information from the target victim, then start the attack. According to the survey, about 88% of clicking links within email of all reported phishing. Whereas most common phishing attacks are happening in financial institute. It is actually difficult to estimate about how much email is sent every day.

But it is reported that 90% of email is spam or virus. Despite the general concept of social engineering is a kind of art that will convincing people to reveal confidential information. The most common target of social engineering attacks happened on help desk officer, technical support executive, system administrator etc. A malicious person is dependent on the fact that people are actually unaware of these values or something careless about protecting the information [1]. The great impact happening by the attacks in any organization. That is economic loss, company or business venture will loss their trust with the customer. So, company want earn much profit due to this attacks. It is the meaning of closing the company or goes for legal fighting. The final result of social engineering attacks is to gaining information that means any kind of privacy will be leak out.

Therefore, to maintain the security of information or information assets is vital for the survival for many organization in doing continuously business [2]. For the artificial intelligence enabled social engineering attacks, the major risk factors are vulnerability and threat. For this reason company should be aware about this risk factor [3].

Literature Review

When the machine will learn the behavior of social network behavior. The artificial hacker will be the subsequent better than normal human performance. Artificial hacker will distribute more phishing mail than human and with the subsequently better rate. One of the artificial intelligences named SNAR_R has sent phishing mail to 890 used with 7.75 per minute. But for normal used it is not possible to spread such an amount. If the AI is used to spread such an amount. If the AI is used for the good use of human then actually no problem at all. But the problem occurs when malicious human being set the AI to gain access to other system without legal permission [4-6].

Whereas social engineering is a discipline in social science. Which is the influence of popular attitude and the social behavior on a large scale by government, media or private groups. That means at first social at first social engineering words was used in social science. Where influential people was try to badly or wrongly way motivated people. It is unknown, how this social engineering word using in information security world. In the cyber world, there are two color crimes. One is white color crime and another is black color crime. In the case of black color crime it is expected that criminal mind people will do criminal work. But in the case of white color crime, there is an interesting things lying here. Actually their type of people doing criminal work, but sometimes they don't have any necessary to do this kind of information

***Corresponding author:** Khidzir NZ, Global Entrepreneurship Research and Innovation Centre/Centre of Computing and Informatics, University Malaysia Kelantan, Malaysia, Tel: +60 9-771 7000; E-mail: zulkarnaen.k@umk.edu.my

Received December 11, 2018; **Accepted** Febuary 22, 2019; **Published** March 01, 2019

Citation: Khidzir NZ, Ahmed SAAM (2019) An Exploratory Factor Analysis of AI Enabled SE Attacking Risk in Higher Learning Institute. J Mass Communicat Journalism 9: 408.

security crime. It is evident that people who would do computer crime, they are not normal computer user people meaning they are basically very advanced computer user people [7-10].

Now the similarity comes of social engineering. We know in social science, the word social engineering means a person who was very influential .The same things may apply in information security world. Here social engineering referring people who are very advanced in technological and they have ill power [11,12]. By this ill power they are trying to destroy or steal something from and organization or business venture. That is why, organization should control and managing the communication as well as growth of information. Especially for banking sector, they should control the aggressive growth of information security to minimizing monetary losses. Therefore it is clearly showing that it is important to analyze the risk factor. Here this paper showing what is the artificial intelligence enabled social engineering attacking risk factor. As described before that information becomes priceless thing. So, security threats such as phishing, spam, intrusion, worms, sabotage of disgruntled employee and stealing data or information from monetarily gains. It is evident that malicious person make the AI only for monetarily gain. As a matter of fact, the malicious person is not interested on normal people data. In the year 2018 , the Federal Bureau of Investigation (FBI) in a survey shown that 5066 organization found that viruses, spyware, PC theft or other computer related crime is increasing and it would cost U.S business a staggering US 76.5 billion a year (news.cnet.com, 2018). It is evident that similar crime may happen in developing countries and other under developing countries [13-15].

AI Enabled SE Attacking Risk Factors

Risk is the term that is widely used in almost every sector such as economics, management, operation research and engineering. Each field defined their risk in own way. There is no similarity of one field to other field. Henceforth, adopt a particular perspective. But the face of risk always as undesirable events. However risk factor that influenced undesirable event that may occur in any field. In all business organization the value of assets is a very important thing. So, risk always indicates the undesirable event in business organization. However in all case such as exchange rate, interest rate and market price affecting the value of assets [7-9].

In the study of information security, there are many contexts and many face of attacking the component that defined the risk factor. However for artificial intelligence enabled social engineering attacks risk factor consist of threat and vulnerability. Artificial intelligence enabled social engineering attacks is a study of information security. However AI enabled SE threat actions causing influence on information security incidents. Whereas other risk also include such as lack of technological fix. If the technology uses in good purpose, so there won't be a problem but if the machine address security problem, but at the same time can be a weakness of the system. The influence of personal data, information leakage, unauthorized exploitation of intellectual property. Thus threat and vulnerability are two major risk factor that need to determined accurately to reduce the risk of AI enabled SE attacking risk. Whereas AI enabled SE, threat refers to the malicious person made circumstance or events that could have any undesirable impact on business organization (Figure 1).

Whereas vulnerability consist of another kind of AI enabled SE attacking risk. Actually vulnerability showing the weakness of an organization when assets that makes a threat. As shown in Figure 2, the named of vulnerability factors item. It is identified by reading through literature review and the used of factor analysis.

Factor ID	A.I enabled SE threat risk factor items	References
T1	Loss , damage or destruction of assets	[1],[5]
T2	Unauthorized access	[6],[1]
T3	Modification of information	[7],[8],[9]
T4	Regular obligation and legal rules	[13],[20]
T5	Identify theft	[21]
T6	Directly exploit control weakness within the organization	[3]
T7	System error	[4]
T8	Sabotage of disgruntled employees	[1]
T9	Employee unawareness of company assets	[6],[9]
T10	Employee upload information on social media site	[11],[13]
T11	Widespread unauthorized and uncontrolled used of portable devise and transportable computer media	[10],[15]
T12	Severely affect the business survivability of organization	[1]
T13	Unauthorized exploitation of intellectual property (IP) (example :plagiarism etc.)	[5],[22]

Figure 1: Showing the AI enabled SE threat items list.

	Vulnerability Risk Factor	References
V1	Lack of security training and awareness	[1],[5]
V2	Insufficient law enforcement	[12]
V3	Account that is not using	[5],[29]
V4	Mismanagement of organization	[13]
V5	Unawareness of important information	[4]
V6	Disorganized condition	[3]
V7	Lack of security in access control	[5]
V8	Insufficient backup system	[4],[25]
V9	Main system failure	[22]
V10	Disgruntled staff	[1]
V11	Disgruntled service provider	[11],[4]
V12	Lack of Antivirus provider	[8]
V13	System weakness	[16]
V14	Lack of knowledge of assets	[19]
V15	Unreliable level of information protection	[21]
V16	Lack of training	[2]
V17	Ignorance , carelessness and negligence of employee	[4]
V18	Unaddressed service provider	[5],[30]
V19	Poor AI enabled SE attacking awareness	[17]
V20	Lack of Business Continuity management	[23]
V21	Lack of disaster recovery planning	[22]
V22	Frequently changed of business policy	[16]

Figure 2: Showing the AI enabled SE vulnerability list.

Methodology

The questionnaire survey was executed for collecting data [16,17]. Both primary and secondary data is used for constructing the methodology. The treat and vulnerability factor of AI enabled SE attacking risk are Exploratory Factor Analysis (EFA). The Principal Component Analysis (PCA) is used on the items of vulnerability and threat of AI enabled SE attacking with orthogonal rotation (varimax). Finally Cronbach's Alpha coefficient is used to test the items reliability for each AI enabled SE attacking risk factor (Figure 3).

The factor value actually got from several literature reviews. The model would be only discussed AI enabled SE attacking risk factor in the education institute .There are thirteen (13) threats and twenty-two (22) vulnerability factor. The survey questionnaire was distributed and tried to find out most relevant influence factors. However, reliability test are conducted for the items. The survey data were collected after distributing the questionnaire to 110 people who are working in the higher learning institution. Besides this also analysis and discussed the AI enabled SE attacking risk threat and vulnerability factors as well as the result of exploratory factor analysis.

Exploratory Factor Analysis (EFA)

First of all the demographic profiling of respondents included their personal working experience. So, far for this article distributed the questionnaire into higher leaning institution. The questionnaire was asked about the position in the organization, asked about the identity of gender and working experience. After analysis the demographic data

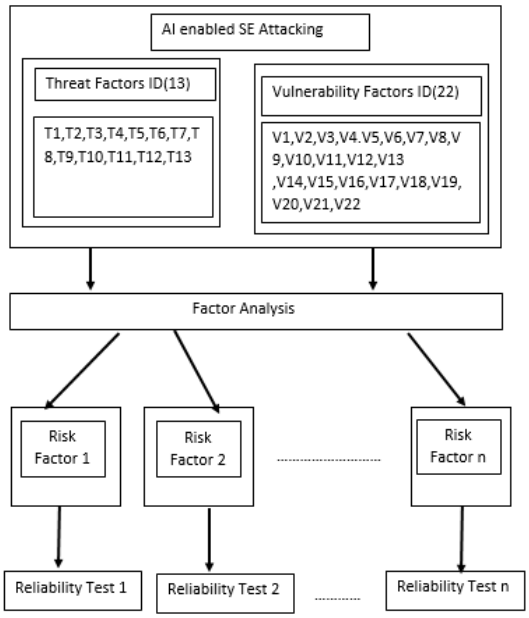

Figure 3: Showing the AI enabled SE attacking threat and vulnerability exploratory factor analysis.

it is shown that in the higher learning institute the response rate of the manger and senior information system officers are 22.3% of the respondents had working experience of 2 to 4 years, the 43% had been working in the institution between 5 to 7 years, however the respond rates of 16.4% are working between 8 and 10 years in the institution, then 13.6% between 11 and 12 years and the rest of only 4.7% engaged more than 13 years working experience in the higher learning institute. Since the questionnaire only distributed in the higher learning institute regarding the AI enabled SE Attacking risk analysis. For the demographic profile in a higher learning institute , were trying to separate the position of respondents , gender were showing the male or female , age of the respondent and personal working experienced in the higher learning institute (Figure 4).

It is seen that from the graph regarding the AI enabled SE attacking risk factor questionnaire. In the higher learning institute data is the most important things. The employee has been working from 2 to 4 years experienced and has shown that their response rate was 22.3%, then from 5 to 7 years of the experienced employee has 43% response rate. Whereas 8 to 10 years experienced, employee has response rate of 13.6%. Nevertheless, more than 13 years of experience employees have respondent rate 4.7%. So it was evidenced that employee has been working 5 to 7 years which having good response rate (Table 1).

Shown that 43% is the highest response rate of the questionnaire. Here in this article conducting statistical analysis technique for the factor analysis of the data. So this how explaining the theoretical structure of the questionnaire. After the identifying the structure of the relationship between the variable of data and the respondent of higher learning institute. As a matter of fact KMO and Bartlett's test are the best analysis technique for this article. Well, this is actually rotation of sums squared loading and rotated the component of the matrix. Now Table 2 is showing the result of the Exploratory Factor Analysis (EFA). After analysis various literature review, finding out the total 35 variables of item (threat and vulnerabilities)with orthogonal rotation (varimax).

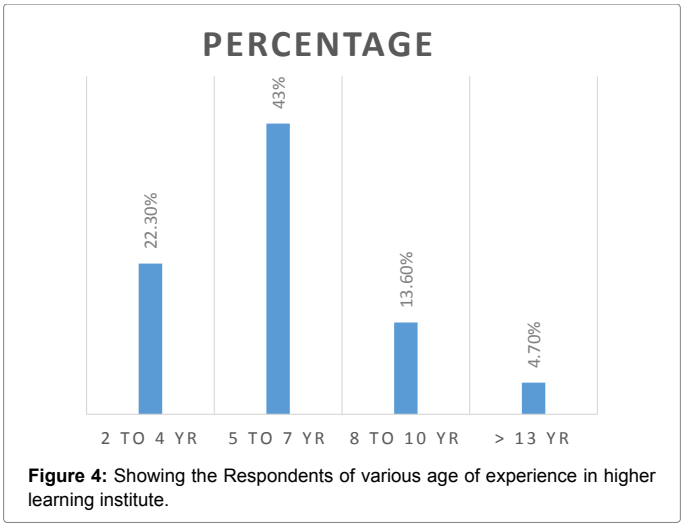

Figure 4: Showing the Respondents of various age of experience in higher learning institute.

Cronbah's Alpha	Number of items
0.920	34

Table 1: Showing the Cronbah's Alpha Value.

KMO Bartlett's test		
Kaiser-meyer-olkin measure of sampling adequacy		0.829
Baetlett's test of sphericity	Approx. chi-square	2622.863
	df	561
	Sig.	0.000

Table 2: Result Summary of Threat Items.

Kaiser-Meyer-Olkin (KMO) measurement is doing here, only to find the sampling adequacy of threats and vulnerabilities. And Bartlett's test is doing for sphericity of variable threat and vulnerability that is based on questionnaires. These two measurement are very important to conclude the worthiness of factor analysis for higher learning institute. As stated that KMO values is between 0 and 1. So, the value of 0 indicated the sum of partial correlation is large relative to the sum of correlations, indicating discussion in the pattern of correlation and the factor analysis is not appropriate to the conducted [18-21]. A value close to 1 indicates that patterns of correlations are relatively compact and so factor analysis should yield distinct and reliable factors. In other words, KMO indicates the amount of variance shared among the items designed to measure a latent variable when compared to the shared with the error recommends accepting values greater than 0.5 as acceptable. More specifically, values between 0.5 and 0.7 are conceded mediocre, values between 0.7 and 0.8 considered good, values between 0.8 and 0.9 are deemed great and values 0.9 are superb [22-25].

From the reliability calculation of the thirty four items it was seen that the Cronbach's alpha value was 0.920, which was showing the most acceptable value of the variable analysis.

Now another the reliability test of Threat and vulnerability factors. From various literature review, got 13 Threat factors and 22 vulnerabilities factor and questionnaire were distributed into higher learning institute. The Kaiser-Meyer-Olkin Measure of sampling adequacy was 0.828, then Bartlett's test of Chi-Square was 2622.863, sphericity difference was 561 and the significance difference was 0.0000 that means we can reject the null hypothesis. It was evidence that every value is reasonable. So there was the validity of the questionnaires.

Since question was distributed to higher learning institute among 110 person, they had demographic difference and different gender [26-28]. And the response rate was 87, and it was shown that 79.09% of the response rate, which was very much acceptable (Table 3).

The result for AI enabled SE attacking risk factor that was derived from the risk factors analysis. Questionnaires consist were 45 items that clustered on risk factor such as Th1, Th2 etc, which was identified by threats [29,30]. The factor loading value would be classified into three categories such as –

<0.7 would represents strong

<0.4 would be representing moderate

>0.4 would be weak

Imposition of legal and regulatory obligation, shown that the value of Th1 is 0.827 the loss, damage or destruction of assets. It was good the respondents were aware about the institutional assets and any kind of data loss. Unauthorized access (Th2), the value was 0.840 which was showing the good response rate among the employees. Now illustrating the selected factors among the questionnaire responses to degree of relevancy (Table 4).

Based on factors analysis results vulnerabilities remain one of the factors that has a contribution regarding the AI enabled SE attacks in higher leaning institute. However from the distribution of questionnaire it is evident that about 11 items cluster on the strong risk application account they are – for the theats factors: Loss, damage or destruction of assets (Th1) (0.827), Unauthorized access (Th2) (0.840), Modification of information (Th3) (0.825), Employee unawareness of company assets (Th9) (0.858). And about 11 items cluster on the strong application are for the vulnerability factors, they are – unawareness of important information (Vul5) (0.855), Disorganized condition (Vul6) (0.843), Disgruntled service provider (Vul11) (0.853), Lack of training (Vul16) (0.824), unaddressed service provider (Vul18) (0.872), lack of Business continuity management (Vul20) (0.816), lack of disaster recovery planning (Vul21) (0.812).

Variable Factors	Loading Risk Factor
Th1	0.827
Th2	0.840
Th3	0.825
Th4	0.791
Th5	0.796
Th6	0.655
Th7	0.808
Th8	0.607
Th9	0.858
Th10	0.796
Th11	0.679
Th12	0.716
Th13	0.731
Vul1	0.793
Vul2	0.777
Vul3	0.824
Vul4	0.780
Vul5	0.855
Vul6	0.843
Vul7	0.784
Vul8	0.721
Vul9	0.760
Vul10	0.750
Vul11	0.853
Vul12	0.793
Vul13	0.691
Vul14	0.770
Vul15	**0.648**
Vul16	0.824
Vul18	0.872
Vul19	0.597
Vul20	0.816
Vul21	0.812
Vul22	0.798

Table 3: Exploratory Factor Analysis (EFA) Result Summary of Threat Items.

Items	Threats and vulnerabilities rotated factor loading	Degree of relevance items
Th1	0.827	Strong +ve
Th2	0.840	Strong +ve
Th3	0.825	Strong +ve
Th9	0.858	Strong +ve
Vul5	0.855	Strong +ve
Vul6	0.843	Strong +ve
Vul11	0.853	Strong +ve
Vul16	0.824	Strong +ve
Vul18	0.872	Strong +ve
Vul20	0.816	Strong +ve
Vul21	0.812	Strong +ve

Table 4: Threats and vulnerabilities rotated factor loading and degree of relevance items

Conclusion

Information security is the combination of people, process and technology. Among them social engineering attacks is a part of study in information security. Whereas the three types of social engineering in information security are – human based social engineering, mobile based social engineering and computer based social engineering. This article only followed artificial enabled social engineering attacks that mean it would cover mobile based social engineering and computer based social engineering. However in artificial enabled social engineering attacks involved potential risks that need to be managed and considered effectively. Serious consideration of the artificial enabled social engineering risk factors is thus required in order to ensure the success running of higher learning institute. To this end it is proved that the finding this study provide the much needed empirical evidence of artificial enabled social engineering attacking risk factors arising from such ventures. An Exploratory Factor Analysis (EFA) was used to identify artificial enabled social engineering attacking risk factors involved in higher learning institute. Results of the analysis show that the threats and vulnerabilities risk factors were extracted in higher learning institute. Finding out that there are three threats factors which are shown strong response form the respondent. That man among thirteen threat factors they are shown important from the respondent. And among twenty-two vulnerability factors there are seven factors which shown strong response from the respondent. So, drawing upon this study, information security specialist should give more concentration on the artificial enabled social engineering threats and vulnerability factor for the security of the higher leaning institute.

References

1. Khidzir NZ, Mohamed A, Habibah Arshad N (2010) Information security risk factors: Critical threats vulnerabilities in ICT outsourcing. International Conference on Information Retrieval and Knowledge Management (CAMP), IEEE Xplore Digital Library.

2. Warkentin M, Willison R (2009) Behavioral and policy issues ininformation systems security: The insider threat. Eur J Inf Syst 18: 101-105.
3. Haley CB, Moffett JD, Laney R, Nuseibeh B (2006) A framework for security requirements engineering. Proceedings of the 2006 international workshop on Software engineering for secure systems, China, pp: 35-42.
4. Whitman ME, Mattord HJ (2011) Principles of information security.
5. Sarkar KR (2010) Assessing insider threats to information security using technical, behavioural and organisational measures. Information Security Technical Report 15: 122-133.
6. Tankard C (2011) Advanced persistent threats and how to monitor and deter them. Network Security 2011: 16-19.
7. Dubois É, Heymans P, Mayer N, Matulevičius R (2010) A Systematic Approach to Define the Domain of Information System Security Risk Management. Intentional Perspectives on Information Systems Engineering pp: 289-306.
8. Autry CW, Michelle Bobbitt L (2008) Supply chain security orientation: conceptual development and a proposed framework. The International Journal of Logistics Management 19: 42-64.
9. Modarres M (2016) Risk analysis in engineering: techniques, tools, and trends. CRC Tylor and Francis.
10. Keeney M, Kowalski E, Cappelli D, Moore A, Shimeall T, et al. (2005) Insider threat study: Computer system sabotage in critical infrastructure sectors.
11. Dutta A, McCrohan K (2002) Management's role in information security in a cyber economy. California Management Review 45.
12. Popović K, Hocenski Ž (2010) Cloud computing security issues and challenges. International Journal of Computer Networks 3.
13. Jacobs S (2015) Engineering information security: the application of systems engineering concepts to achieve information assurance. (2ndedn) John Wiley and Sons.
14. Farahmand F, Navathe SB, Sharp GP, Enslow PH (2005) A management perspective on risk of security threats to information systems. Information Technology and Management 6: 203-225.
15. Garfinkel S, Spafford G, Schwartz A (2003) Practical UNIX and Internet security, (3rdedn). O'Reilly Media.
16. O'RourkeTD, Briggs TR (2007) Critical infrastructure, interdependencies, and resilience. The Bridge 37.
17. Mayer N, Heymans P, Matulevicius R (2007) Design of a Modelling Language for Information System Security Risk Management. pp: 121-132.
18. Workman M (2007) Gaining access with social engineering: An empirical study of the threat. Information Systems Security 16: 315-331.
19. Parker DB (1995) A new framework for information security to avoid information anarchy. In: Eloff J.H.P., von Solms S.H. (eds) Information Security — the Next Decade. IFIP Advances in Information and Communication Technology. Springer, Boston, MA, pp: 153-164.
20. Laorden C, Sanz B, Alvarez G, Bringas PG (2010) A threat model approach to threats and vulnerabilities in on-line social networks. Proceedings of the 3rd international conference on computational intelligence in security for information systems (CISIS'10) pp: 135-142.
21. Salini P, Kanmani S (2012) Survey and analysis on security requirements engineering. Journal Computers and Electrical Engineering 38: 1785-1797.
22. Peltier TR (2010) Information security risk analysis. (3rdedn) Auerbach Publications.
23. Bojanc R, Blažič BJ (2013) A quantitative model for information-security risk management. Engineering Management Journal 25: 25-37.
24. Herrmann DS (2001) A practical guide to security engineering and information assurance. Auerbach Publications
25. Stanton JM, Stam KR, Mastrangelo P, Jolton J (2005) Analysis of end user security behaviors. Computers & Security pp: 1-10.
26. Foster HD (2012) Disaster planning: The preservation of life and property. Springer Series on Environmental Management
27. Tops Documentation, C Logical (2005) Information technology–Security techniques–Information security management systems–Requirements. International Organization for Standardization.
28. Blyth A, Kovacich GL (2006) What is Information Assurance?
29. Onwubiko C, Lenaghan AP (2007) Managing security threats and vulnerabilities for small to medium enterprises.Conference proceeding in Intelligence and Security Informatics.
30. Jerman-Blažič v (2008) Towards a standard approach for quantifying an ICT security investment. Computer Standards & Interfaces 30: 216-222.