Journal of Contemporary Issues and Thought
ISSN 0128-0481/ e-ISSN 2232-0032 / Vol 9, 2019 (12-17)

Viewpoint of Probabilistic Risk Assessment in Artificial Enabled Social Engineering Attacks

Nik Zulkarnaen Khidzir[1] & Shekh Abdullah-Al-Musa Ahmed[2]

[1]Global Entrepreneurship Research and Innovation Centre, Universiti Malaysia Kelantan, Bachok, Kelantan, Malaysia
[2]Faculty of Creative Technology and Heritage, Universiti Malaysia Kelantan, Bachok,Kelantan, Malaysia
[1] zulkarnaen.k @umk.edu.my & [2] almusa.c17e002f@siswa.umk.edu.my

Abstract

Risk assessment really a complex decision-making process in the domain of in-formation security areas. There are a lot of unclear model of software domain and the lack of associated uncertainty are two main reasons that directly affect individual decisions making regarding risk assessment. When artificial enabled social engineering attacks are effectively may happening in every levels of domain. On the other hand, the risk assessment conducted on the safety requirements on artificial enabled social engineering attacks. So the simple meaning of social engineering is to refers to the psychologically and mentality use people to give secret information in the context of information security. A strategy of self-confidence for information collection, fraud, or access to the system, is different from a traditional "con" that it is often one of the more complex fraudulent schemes. That is why in this paper we proposed theoretical framework, which can not only demonstrate its potential for the risk assessment, but it can be sensitive and effective in analyzing a critical and uncertain operational environment that can address the extreme effects of information security.

Keywords: Risk assessment; Social engineering; Artificially-enabled; Malicious software; In-formation security; Vulnerability; Artificial enabled social engineering risk; Coun-termeasure

I. INTRODUCTION

Risk assessments for artificially enabled social engineering attacks identify a relevant data resource (risk factors), discover their relationship, and formulate a risk assessment argument to process their integration. Regarding un-certainty, we have to deal with four issues: 1) first we have to understanding about the artificially enabled social engineering attacking risk formula; 2) How are pieces of information integrated (build a causal model); 3) How new information can be included (for model evolution); and 4) what happens when the working conditions change (for the reasons of changed risk and their orientation).

Artificial Intelligence (AI) is the news has recently been in information security area. Some say that artificial intelligence will do human work in the future. Artificial Intelligence have the power to make everyday activities easy (Workman, 2008). However it will take the ability to provide faster information against cyber-attacks, especially social engineering attacks.

Every year, billions of people, and many people did not understand the conversation that is already going on with chatbots. That they are not talking with people. In fact, a bot named The zboy is being used on Facebook and allows businesses to communicate with their customers easily through posting. Even we can see that Amazon's Alexa is now available for help with travel planning, entertainment, decorated products and other various uses. It's

nothing but all about AI working in the information security area .There are other factor of information security is about the malicious activity and identify the activity. In artificial enabled social engineering attacks there is a term malware is often used but is often misunderstood, so let's explain its first meaning. The word malware is malfunctioned for malicious software, which clearly described how the class software is designed, performs harmful and confusing tasks. In the last decade, what we say now is not essential for the nature of malware. It is more damaging the software of this class is infected, interrupted, disabled. Including the operating system, is usually just annoying and annoying system owners. In recent years, however, many more malignant applications included in this software category, that included the current malware and by increasingly complexity.

However the real objective and motivation of this article is to reduce the artificial enable social engineering attacking risk in the information security domain. And showing how the variable factor of social engineering risk such as valuation, countermeasure and vulnerability are related with the artificial enable social engineering risk. As a matter of fact this is the theoretical process to detraining the quantitative approach of artificial enabled social engineering attacking risk process (Major, 2009).

Whereas the papers only described the general process of quantitative approach of risk management process of artificial enabled social engineering attacks in the organizations. So, it may be applied to determine the risk analysis process by distributing the questionnaire in various organization and determine the quantitative approach of risk for artificial enables social engineering attacks in the origination.

II. LITERATURE REVIEW

There are three types of social engineering in information security area. They are – human based social engineering, computer based social engineering and mobile based social engineering. In the case of Artificial Intelligence enabled social engineering, we would like to only consider about the computer based social engineering and mobile based social engineering (Abawajy, 2014). Although the greatest area for success is human-based interaction by social engineers. However there are some computer-based methods that attempt to retrieve data using software programs to recover data or to deny access to a system. One of the most intelligent methods was the first to be launched on the Internet in February 1993. The user attempting to login to the system was given a normal prompt and after entering the correct username and password, the system started again in the prompt order. What happened, was that a social engineer managed to install a program in front of the normal signing routine, gather information and then pass the prompt to the actual signing process. More than 95% of regular users had access to their code of access. Today we can use web sites to see that a common driver provides some free or at least a chance to win a web site or gain important information. In a Michigan firm in 1998, the Network Administrator established a 401K data website, which employs to register employees for the collection of their 401K program information. Account id, password etc. After providing this information as a social security number and home address, the website sent a message that it was still under construction. Almost every employee tries to register on the web site, including senior management, assistant manager and other employees. So this is one kind of social engineering attacks to grab information. Now we can divided the social engineering attacks into two types: human Based and technology oriented. A man-based person refers to person-to-person interaction for which

desire is to be spent. Artificial intelligence refers to having an efficient-based electronic interface that strives to recover the expected results.

III. ARTIFICIAL ENABLED SOCIAL ENGINEERING ATTACKS :

Let's see what the common artificial enabled social engineering attacks are. Here actually human spoil the system, then the system perform differently. If we want to see the meaning of social engineering then we can see that, in social science this word is available. It means a person has strong capability to modify the society and by his ill-power he changed the society wrongly (Clay et al., 2015). This is an old type of crime. Many political leader was involved this type of crime. Later this word come into information security area. Which shows that a person has intelligence and grab the information from other person. In this article we are focus on artificial enabled that is machine based activity regarding social engineering attacks. Such as:

Pop-up Windows: Let's assume that in a computer screen has been showed not connected. Then the pop up program will give an access information. Another program may asked user to submit their user name and personal information. Usually email comes when a malicious person used the credit card and the credit card value is expired. Normally user does nor suspect that the site is faked. This is one kind of phishing scam and it has become much more sophisticated in recent months.

Mail attachments: In the case of mail attachment, malicious person usually send a email to the victim and with the mail, some malicious program will be hidden inside the email. Here the first step is to understand the victim and find out the weakness. After then write a malware program that is kept in-side the mail (Vuorinen, 2013). This is actually one kind of malware called Trojan, which is kept inside the email. So, clicking the email means spreading the malware.

Website: In the situation of website attacks, by social engineering attacker, the malicious person has a trend to send spam and identify the theft that is a new trend in security area and is called spoofing. The malicious per-son sending the email to the victim. Showing the mail that a legitimate initiative user has to do something. This is actually phishing or brand phishing activity. The common goal of this type of malicious person is – government office, health care, bank and educational institution. The malicious person send an email to fill up a form with a fraudulent copy of an existing webpage via the victim email.

IV. METHODOLOGY

In this section, the methodology of the article is discussed .Also describing the re-search framework, data collection and analysis process of AI enabled SE attacking risk factors.

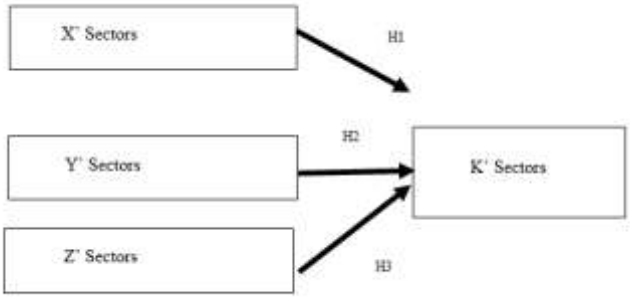

Figure 4.1: Showing the Research Framework

A. Theoretical framework and Hypothesis

The probabilistic risk assessment type of questionnaire survey could be applied in this research. In that case, would using both primary and secondary data. That will be used in order to accomplish this getting numeric risk value for the assessment.

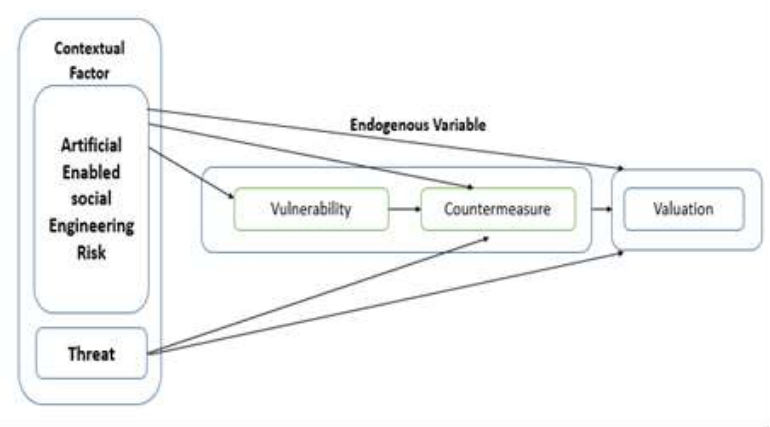

Figure 4.2: Theoretical framework for Analysis Model

In the figure 1 described the research model of our study, accordingly to the literature review, it is hypothesized that:

Hypothesis 1: Artificial Enabled social engineering risk (AISER) will have a positive effect on the valuation (Val).
Hypothesis 2: Countermeasure (Cms) mediated the relationship between artificial enabled social engineering risk (AISER) and valuation (Val).
Hypothesis 3: Vulnerability (Vul) mediated the relationship between artificial enabled social engineering risk (AISER) and valuation (Val).
Hypothesis 4: Vulnerability (Vul) and Countermeasure (Cms) mediated the relationship between artificial enabled social engineering risk (AISER) and valuation (Val).
Hypothesis 5: Threat (Th) factor will have a positive effect on valuation (Val).
Hypothesis 6: Countermeasure (Cms) mediated the relationship between Threat (Th) factor and valuation (Val).
Hypothesis 7: Vulnerability (Vul) and Countermeasure (Cms) mediated the relationship between Threat (Th) factor and valuation (Val).

V. THE REQUIREMENTS OF PROBABILISTIC RISK ASSESSMENT FOR AISER

We know the domain of risk assessment is totally uncertain in that case an effective decision must be take against artificial enabled social engineering risk and decision must be made by answering the question. For example – How likely a certain threat (Th) is occurred? or How effectively a countermeasure for AISER can mitigate certain vulnerability ? etc. Since probabilistic reasoning technique are widely used in information security domain. Certain number of interrelated hypothesis and have the ability of combining qualitative expert knowledge with quantitative measure of statistical data. In the figure 1 shows that artificial intelligence enabled social engineering risk and threat are contextual variable. In the information security world, every person in under a threat. Because we all are connected by

internet (Hinson, 2008). Any type of malware attacks may happened, but malicious person are interested about financial data. They will be more benefited by analysis of financial data. The proposed framework and their properties are related to risk assessment, such as countermeasure and as well as threat. For the probabilistic risk assessment we are proposing the formula.

$$\text{Probabilistic Risk Assessment} = \frac{\text{Artificial intelligence enabled social engineering risk(AIESER)}}{\text{Loss if event occur}}$$

VI. MOTIVATION AND BENEFITS

Based on the theoretical framework, domain expert will identity the relevant risk component and using this concept they will map the specific artificial intelligence enabled social engineering risk. It is true that we are producing more and more information and organizing them to seek better ways to extract knowledgeable. So turning towards the advances in artificial intelligence. This is the technology that come to help in many aspect of life such as simple machine learning, that indicating to purchase more practical uses such as in Data Security and financial prediction or speculation .By using the probabilistic risk assessment, we can determine the risk matrix (Pieters, 2011). Artificial intelligence is giving good motivation of society. In everyday life we are using machine. That's actually good turning. But the challenge will come, when human begin using this machine in bad purpose. Actually referring about cyber-crime. So, Trojan horse is one kind of malicious computer program which is used by social engineering activity (Tham et al., 1991). Though there are several ways to get prevention from Trojan horse malware attacks. However in this paper, we are proposing a theoretical frame-work to mitigate the risk from this kind of attacks. The main benefit of this qualitative framework is when knowing the value of which sector is under risk, then can give more protection on this sector.

VII. CONCLUSION AND FUTURE DIRECTIONS

The probabilistic risk assessment value must be within 1 (one). Once organization would get the artificial enabled social engineering risk value which would be divisible by expected loess (if any artificial enabled social engineering attacks may happen). Both value would be quantitative value. And the end result would be probabilistic risk assessment, which value would be within 1(one). By calculating different department , different probabilistic risk assessment , organization would send this result to head of information security officer to take further protection from this information security attacks in the organization.

For the decision making process or for many kinds of activity, may create a map to reach our destination. This paper focus on how artificial intelligence enabled social engineering attacks are threat to individual or organization. The theoretical framework are the components a and the relationship of the components .Though in information security to mitigating risk is a very important factor. Even we cannot properly reduced our risk (Buang et al., 2012). But any kind of statistical approach for quantitative analysis is also very important things. In this paper, proposing probabilistic risk assessment formula which will employed in the risk assessment of artificial intelligence enabled social engineering attacks. The risk assessment probability will point out a report phrase for risk matrix. Now we can understand, artificial intelligence can be used to defend and to attack in cyber world. Even today it is increasing the attack surface, that innocent victims targeted. A number of ways a malicious person can get

into the system, which has been described in the paper. For example the game like chess. It is important to the individual as well as organization owner to understand how the future situation may happen by the artificial intelligence enabled social engineering attacks .The ultimate situation will be someone will loss his money or privacy. The risk are real, as evidenced by fact, so it is relevant to construct a theoretical framework against the attacks.

VIII. REFERENCES

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

Buang, M. F. M. E. A. & Daud, S.M. (2012). A web-based KM system for digital forensics - Knowledge sharing capability. Proceedings of 2012 International Conference on Multimedia Computing and Systems, ICMCS 2012, Pages 528-533.

Clay Posey, T. L. R. P. B. L. (2015). The Impact of Organizational Commitment on Insiders' Motivation to Protect Organizational Information Assets. Journal of Management Information Systems, Volume 32(Issue 4), Pages 179-214.

Hinson, G. (2008). Social Engineering Techniques, Risks, and Controls. The EDP Audit, Control, and Security Newsletter, Volume 37(Issue 4-5), Pages 32-46.

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

Pieters, W. (2011). The (Social) Construction of Information Security. The Information Society, Volume 27(Issue 5).

Vuorinen, P. T. J. (2013). Dissecting social engineering. Journal Behavior & Information Technology 32(10), Pages 1014-1023.

Workman, M. (2008). Wisecrackers: A theory-grounded investigation of phishing and pretext social engineering threats to information security. Publication cover image Volume59, Issue4, 551-564.

Tham, M. T., Vagi, F., Morris, A. J., & Wood, R. K. (1991). On-line multivariable adaptive control of a binary distillation column. Volume 69(Issue 4), 997-1009.