Proceedings of the International Multiconference on Computer Science and Information Technology pp. 847–853
ISBN 978-83-60810-27-9
ISSN 1896-7094

Social Engineering-Based Attacks: Model and New Zealand Perspective

Lech J. Janczewski
The University of Auckland, New Zealand
Email: lech@auckland.ac.nz

Lingyan (René) Fu
The University of Auckland, New Zealand
Email: reneweiss14@gmail.com

***Abstract*— The objective of this research was to present and demonstrate the major aspects and underlying constructs of social engineering. An in-depth literature review was carried out resulting in the construction of a conceptual model of social engineering attacks. A case study was undertaken to understand the phenomenon with New Zealand-based IT practitioners to contribute insightful opinions. On this basis an improved model of social engineering-based attacks was formulated.**

I. Introduction

IN THE context of information security, social engineering describes a method of launching attacks against information and information systems. Both organizations and individuals have suffered enormous loss from these attacks. However, social engineering as a security threat is constantly overlooked because awareness of this phenomenon is currently low and there is a lack of a conceptual model to represent this form of attack.

The objective of this research was to present and demonstrate the major aspects and underlying constructs of social engineering and identify the relations between them. An in-depth literature review was carried out resulting in the construction of a conceptual model of the social engineering attacks.

A case study was undertaken to understand the phenomenon and a total of twenty-five New Zealand-based IT practitioners participated in this research to contribute insightful opinions.

Analysis of the collected opinions allowed us to present an improved model of social engineering-based attacks.

The paper starts with the formulation of the research objective and hypotheses followed by a presentation of a literature-based model of these attacks. Analysis of the New Zealand-based researchers' opinions is then presented. The paper terminates at the formulation of an improved model of social engineering based attacks.

II. Research objective, working hypotheses and methodology

The overall research objective of this study was defined as:

Exploring the significant entities and relations within social engineering-based attacks

To properly address this research objective, we formulated the following specific research questions:

RQ1: *What are existing security vulnerabilities which can be exploited by social engineering based-attacks?*
RQ2: *What are the methods of social engineering-based attacks?*
RQ3: *What are the consequences of a successful social engineering attack?*
RQ4: *What can be done to mitigate Social Engineering-based attacks?*
RQ5: *What is New Zealand's perspective of social engineering-based attacks?*

An exploratory case study approach was chosen to conduct the research investigation.

III. Proposed Model

Based on analysis and discussion of the conducted literature review, several key entities of social engineering attacks have been identified: People, Security Awareness, Psychological Weaknesses, Technology, Defenses, and Attack Methods.

As shown in Table 1, hacking and social engineering are the most common attack methods adopted across most fields. Traditional hacking and malicious code attacks are technical-based, targeting system or application vulnerabilities. However, the effectiveness of technical-based attacks has decreased as technological security solutions are gradually being adopted by more and more people and organizations [1]. Hence, this has encouraged technical hackers to choose the alternative – social engineering, targeting the existing vulnerabilities of both people and technology [2]. As a result, it is considered as the biggest security threat faced by both organizations and individuals today.

Social engineering is a diverse and complex technique for gaining unauthorized access to confidential proprietary and personal information [3]. It is primarily known as non-technical (human-based) attack, including impersonation, dumpster diving, shoulder surfing, and reverse social engineering; however, it could also be technology-based, including pop up applications, email attachment, online scams, and vishing. The literature review also indicates that the trend of technology-based attack is increasing with the emerging Internet technologies, such as online services and social networks [4], [5], [6] and [7].

IV. Consequences

The impact of social engineering attacks can be significant to both individuals and organizations [3]. The phase of the attack decides the type of information that may be valuable to social engineers. For instance, at the information gathering stage, information such as miscellaneous trivia within an organization; internal documents such as phone directories and organizational charts can be very useful. From an individual perspective, it will be personal information, such as date of birth, address and so on. Loss of CIA is the lesser damage and seen as the

Table I.
Summary of Security Threats and Attack Methods

Threat Initiator	Motivation	Attack Action	Method
Hacktivism (hacker, cracker, Phreaker, script kiddies)	• Ego, fame • Destruction of system or information	• DoS / DDoS • System intrusion • Website defacement • DNS attack	• Hacking • **Social engineering**
Computer Criminal	• Theft of data • Monetary gain • Privacy compromise • Illegal information disclosure • Unauthorized data alteration	• Cyber stalking • Fraudulent act (man-in-the-middle, spoofing)	• Hacking • **Social engineering**
Insider (disgruntled, poorly trained, dishonest, malicious, negligent, former employee)	• Revenge • Monetary gain • Intelligence	• Unauthorized access • Computer abuse • Fraud • Theft of proprietary information (both logical and physical) • Bribery • System sabotage	• Malicious code (logic bomb, Trojan, malcode inserted as part of the software development process) • **Social engineering**
Industrial Espionage	• Competitive advantage	• Unauthorized access • Information theft • System Penetration	• Hacking • **Social engineering**

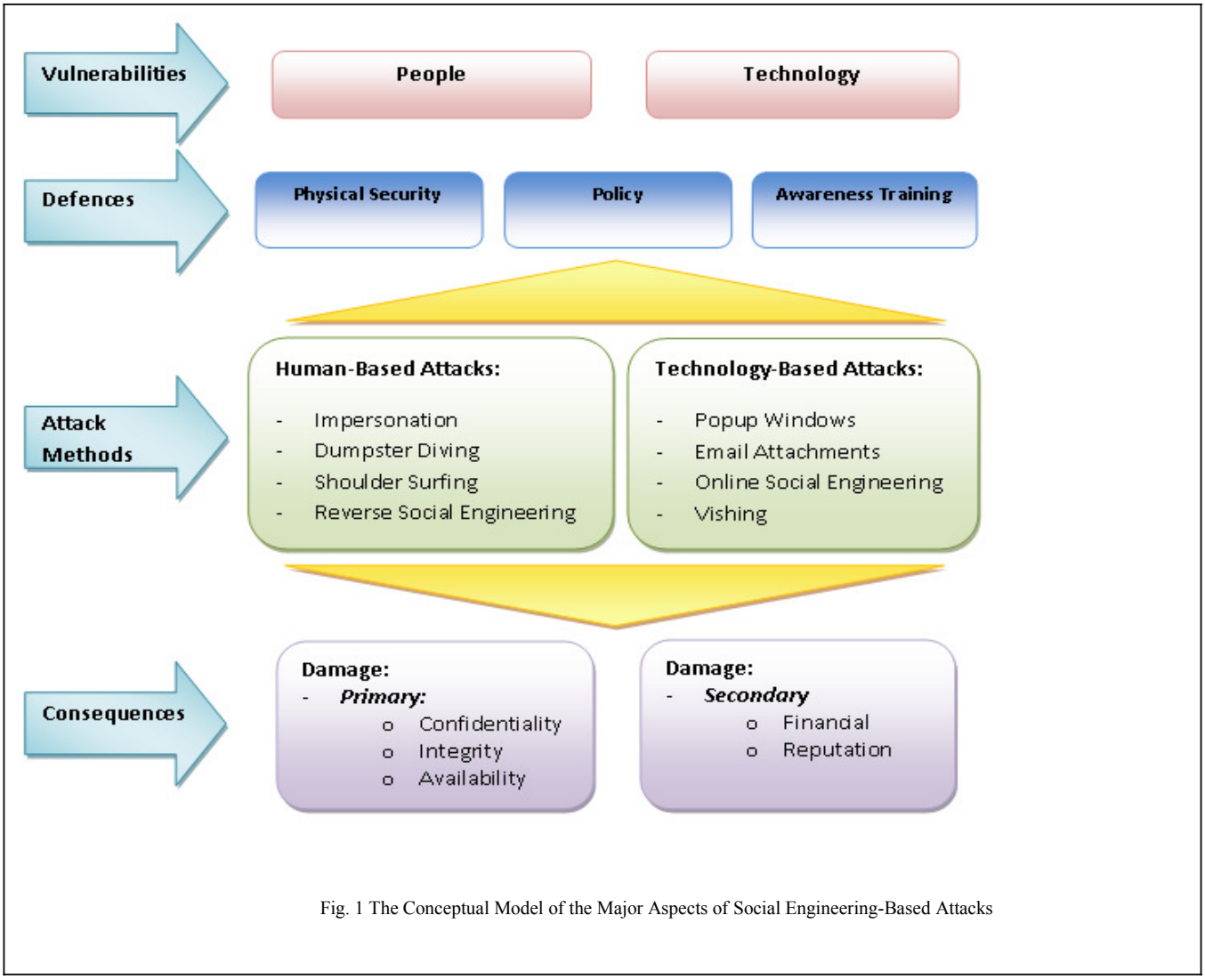

Fig. 1 The Conceptual Model of the Major Aspects of Social Engineering-Based Attacks

TABLE 2
SIX ENTITIES USED FOR DATA ANALYSIS

Entities	Description
People	Vulnerabilities in people that can be exploited by social engineering-based attacks.
Technology	Vulnerabilities in technology that can be exploited by social engineering-based attacks.
Security Strategy	Vulnerabilities in security strategy that can be exploited by social engineering-based attacks.
Defenses	Possible defenses to mitigate the risk of social engineering-based attacks.
Attack Methods	Types of the common social engineering-based attack methods.
Consequences	The damage of social engineering-based attacks to both organizations and individuals.

primary result of a successful social engineering attack. The information gathered is later used in the subsequent stage - attack phase. Again depending of the purpose of the attack, the level of damage varies. This is considered as the secondary damage of successful attacks.

The secondary damage is twofold. From a commercial perspective, firstly, social engineering attacks may cause significant financial losses, for instance, loss of business secrets to the competitor as a result of an insider attack, or loss of important equipments as a result of physical attack. Secondly, public disclosure of sensitive customer information stolen from a financial institution will damage the organization's image, followed by subsequent financial loss. From an individual's perspective, social engineering is a threat to people's personal life and finance, for instance, bogus advertisement and phishing attacks are the typical examples. The direct consequence to these attacks is identity theft which will finally lead to financial damage.

The above major entities form the basis of the social engineering-based attacks model presented in Figure 1.

V. DATA ANALYSIS & FINDING

To verify the proposed model a total of 25 interviews were conducted, and the participants (from 17 organizations) were of various IT related backgrounds and experiences. The organizations the participants work for are across industries, including financial institution, security advisory services, government department, IT advisory, IT outsourcing, multi discipline computer firms, multi discipline consulting firms, and education. Among these organizations, there were seven local organizations and ten international organizations. The participants' job functions can be largely divided into seven categories: IT advisor, IT architect specialist, IT consultant, security specialist, IT solution designer, database management, and IT educator.

The entities used for the interview were derived from the conceptual model proposed in Fig.1 and summarized in Table 2. Major findings are presented next while the detailed answers are in [8].

VI. THE REFINED MODEL

Based on previous discussion and analysis of the information gathered during the interview phase, the revised model was developed shown in Fig 2. In the "Vulnerabilities" section, Security Strategy is added as a new entity which emerged from the analysis of the twenty-five conducted interviews. Security Strategy is in place to eliminate existing risks; however, the result from the interview analysis suggests that immature security strategy can be exploited indirectly by social engineering-based attacks. Therefore, Security Strategy is also considered as a vulnerable entity in information security. In the "Defenses" section, Technical Controls, Security-Enhanced Products, and Education entities were added.

These are the additional defence approaches which were believed to improve the mitigation of social engineering risks. In the "Attack Methods" section, Questionnaires are added as a new information gathering method.

Answering the research questions presented at the beginning of the paper:

RQ1: *What are existing security vulnerabilities which can be exploited by social engineering based-attacks?*

This research question was answered by findings from both the literature review and data analysis. The literature review identified two major components in information security that can be directly exploited by social engineering, including people and technology. In agreement with the literature review, the interview analysis suggested that security process should also be considered as a component which is vulnerable to such attacks.

Both the literature review and data analysis have suggested that people are the weakest link in security control systems. In addition, lack of security awareness and psychological weaknesses of people are the main reasons that social engineering-based attacks succeed. According to the literature review, people lack understanding of the current security issues - especially social engineering. This is supported by **64%** of the interview participants. Secondly, in agreement with the identified psychological weaknesses from the literature review, **40%** of the participants commented that appearance is a significant factor that can influence people's perceived trustworthiness.

The findings have suggested that there are three major issues associated with technology. First, the literature review has revealed that a lot of technology products have flaws in the security design. These flaws are used by an attacker to generate technology based scams which preys on people's fear of security. Data analysis shows that **16%** of the participants agreed to this. Secondly, in line with the literature review, **12%** of the participants pointed out that most security technologies are incapable of detecting and preventing social engineering as social engineering bypasses technical controls via manipulating people who are managing them. Additionally, **12%** of the participants stated that there is an increasing trend of malicious misuse of advancing technology products, such as Google Applications. It was also noted that online social networking services are often used as information gathering tools by the social engineers.

From the data analysis, security strategy emerged to be a significant entity that is vulnerable to social engineering-based attacks. The literature review has suggested that social engineering depends on uncertainty, for example, people are unsure about the requestor's identify, or people are

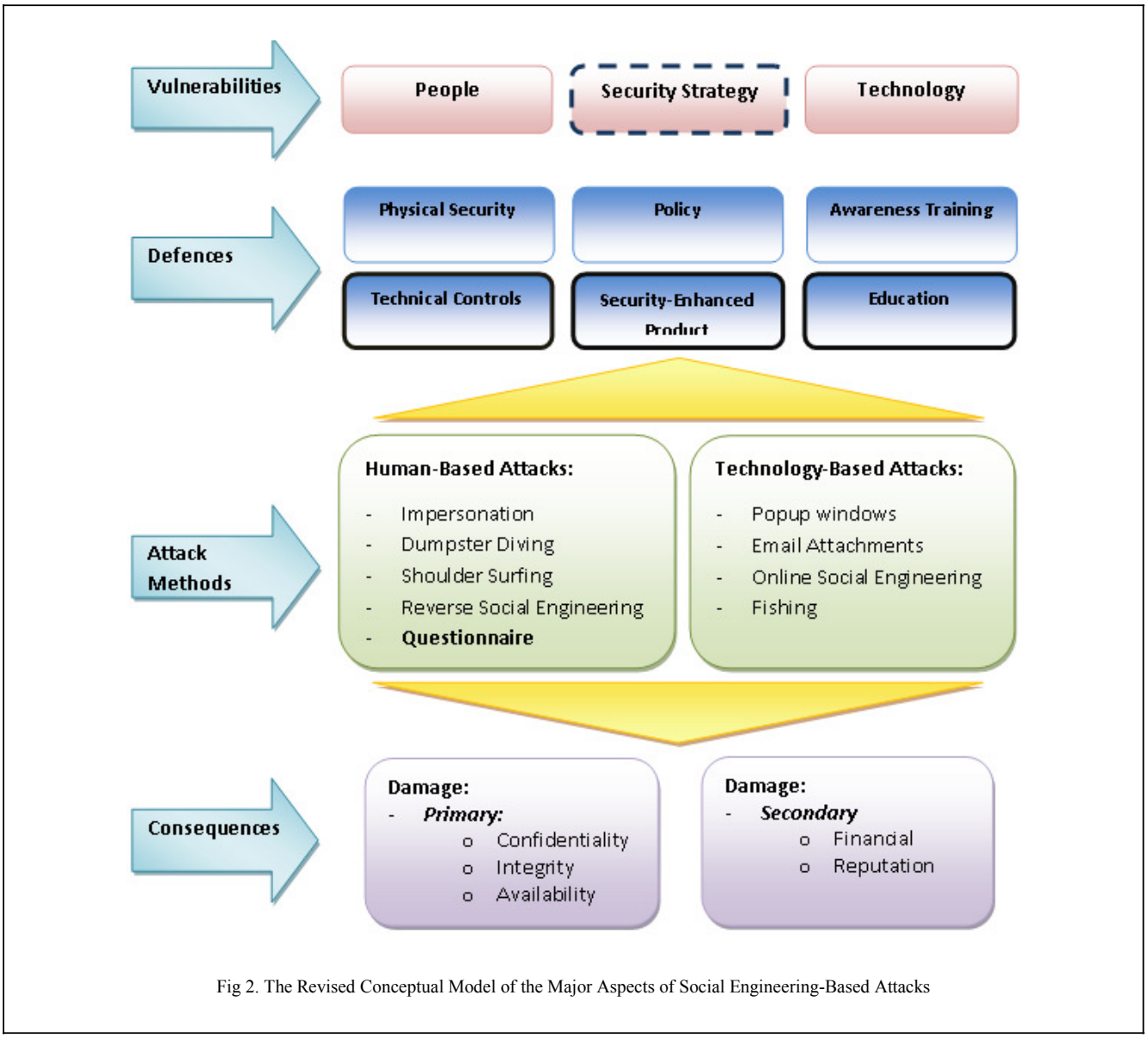

Fig 2. The Revised Conceptual Model of the Major Aspects of Social Engineering-Based Attacks

unsure about if it is the right thing to grant access to the requestor, etc. This is the main reason for putting in place a well-thought-out security strategy. However, **40%** of the interviewed participants emphasized that in general security strategies of organizations in New Zealand had poor security strategies because they overlooked people issues. Four types of threats from ineffective security strategies resulted from the data analysis - human behavior, system types of threats from ineffective security strategies resulted from the data analysis - human behavior, system implementation, physical environment, and governance issues. As the interview participants pointed out, a prospective social engineer may launch attacks against any of these vulnerabilities and conduct successful attacks.

RQ2: *What are the methods of social engineering-based attacks?*

Social engineering is often referred to as the people side of hacking which relies on influencing, deceiving, and psychological manipulation with or without the use of technology. It is diverse and complex and the form of the attack varies based on the attack motivation. Today, social engineering-based attacks can be basically classified into two categories, including human-based and technology-based.

Human-based social engineering is purely based on deception and can be conducted either in person or over the telephone. The methods include impersonation, dumpster diving, shoulder surfing, reverse social engineering, and questionnaire. Also, compared to an in person attack, by telephone is the most widespread mode as voice can be disguised. This mode is also easier for the social engineers to cover their tracks.

Technology-based social engineering is closer to traditional hacking technique. The purpose is to trick users into believing that they are interacting with authentic computer systems through the use of software or application. The attack methods include popup windows, email attachments, online social engineering, fishing, and rogue security software.

RQ3: *What are the damages after the attacks have been launched successfully?*

TABLE 6
ANALYSIS OF PARTICIPANTS' SOCIAL ENGINEERING-BASED ATTACK EXAMPLES

Attack Method	Case #	Description	Damage
Dumpster Diving	**Case 1**	The attacker went through waste to discover useful information such as credit card number simply because the merchant didn't pay attention to their waste management.	The victim lost their confidential information and money.
In Person	**Case2**	The pen-tester pretended to be someone who worked on the management floor and made the cleaner believe him. The cleaner had full access to the building, yet, their security awareness is very low. They are not trained to respond to unusual request.	It is only a penetration testing for the company, therefore nothing was lost.
	Case3	The attacker impersonated a cleaner to plant the key logger to steal sensitive information.	There was no significant damage because that bank has adopted appropriate security controls.
	Case4	People got access to the building and stole company property during office hours simply because the office staffs don't challenge strangers and abnormal behaviours.	Company equipment got stolen; this is considered as a financial loss.
	Case5	Similar to the previous pen-test case, the pen-tester was able to bypass security controls and gain access to company resources because the internal staffs, such as the reception was convinced that the pen-tester was part of the company.	It was a penetration testing; therefore there was no real damage.
Online Social Engineering	**Case6**	The attacker built trust with the victims and sent them photos with an embedded Trojan. The victims accepted the photos because their level of security awareness is very low.	The victim lost their confidential information and money.
	Case7	The attacker set up a fake website with full merchant facilities and security certificate to sell bogus Olympic tickets. It was never a business to begin with, yet, the bank and VeriSign didn't validate at all.	A large number of people paid for the ticket that would never get delivered, over 50 million dollars was scammed.
	Case8	The attacker took advantage of the online dating services and tricked a number of female victims. He first chatted with them through email and gradually built trust with them. He then sent them photos with an embedded key logger to steal their bank account details.	Victims lost money.
Telephone	**Case9**	The attacker tricked people over the phone into revealing biometric authentication (voice) pass phrase to use it later at the authentication point.	People's pass phrase got stolen and used for later attacks.
	Case10	The pen-tester pretended to be a customer who knows about the services. He was able to get sensitive information out of the helpdesk by bypassing the normal identify checks. On the other hand, it also showed that there was a lack of training and security awareness in that company.	If it was a real attack, the company may end up losing business confidentiality.
	Case11	A practical test to see how the bank handled abnormal situations. The initiator pretended to be helpless and prey on the customer services' sympathy.	The tester successfully changed the other party's passwords twice. In a real attack, the likely result is money loss.
	Case12	The attacker called the helpdesk and impersonated one of the contractors trying to gain access to the company network. Fortunately, the helpdesk found out and successfully prevented the potential attack.	Nothing happened because the helpdesk was doing their job properly.

The damages of a successful social engineering attack are twofold, primary and secondary. Similar to traditional hacking, social engineers spend most of their time in preparation via information gathering. To do so, the social engineer needs to gain authorized access to resources which leads to a breach of CIA. This is considered as the primary damage if the attack is successful. The information gathered is then used in the subsequent attack phase - the secondary damage.

Secondary damage can be largely divided into two parts, reputation damage and financial damage. The typical social engineering attack targets organizations with sensitive information, such as customer database. Loss and improper disclosure of information will seriously damage the organizations' reputation as well as finances. Moreover, finances may be rebuilt, but people's confidence and positive reputation can take years to rebuild.

RQ4: *What can be done to mitigate Social Engineering-based attacks?*

Social engineering represents a wide range of threats. To effectively defend against social engineering-based attacks, it is necessary to have a multifaceted approach. Firstly, on the very basic level, physical security must be properly implemented because a lot of the attacks are through gaining physical access. Therefore, access control must be in place to

allow the authenticated people to have access while keeping the rest out. Ideally, organizations should apply different access control mechanisms based on the security classification. Secondly, proper technical controls can help to reduce social engineering risks, such as multifactor authentication can effectively prevent unauthorized access, especially for online financial identify theft. Thirdly, security policy is the key and most important element of a good defence against social engineering because it can take out uncertainty which is what social engineering depends on. The policy should include all the business components which are necessary to protect. Ultimately, security policy should be supplemented by education and training. People's vulnerability to social engineering can be described in terms of their awareness to these types of attacks. Therefore, people must be educated and trained constantly to be social engineering resistant.

RQ5: *What is New Zealand's perspective of social engineering-based attacks?*

In general, New Zealand shares a similar trend with other countries in terms of technology adoption and security risks. However, with regards to awareness of security issues and the implementation of countermeasures, New Zealand is a behind others.

First, according to **64%** of the interviewed participants, the majority of businesses and people in New Zealand do not have sufficient understanding of existing security issues. **32%** of them particularly mentioned the social engineering phenomenon is overlooked. The findings show that apart from people's careers, environmental factors (economical scale, legislation, and breach disclosure) also affect people's security awareness. In particular, **28%** of the interview participants mentioned it is mainly because there have not been major security disasters in New Zealand. **8%** of the interviewed participants pointed out that the other reason is the large number of security breaches, especially internal breaches in New Zealand that are underreported due to insufficient law enforcement. In addition, **44%** of the interviewed participants commented that people in New Zealand generally have a higher level of social trust which implies that they are more vulnerable to social engineering-based attacks.

Secondly, with regards to security strategy, **40%** of the interview participants commented that the organizations in New Zealand in general do not have a well-defined security strategy because they overlook people issues. **16%** of them pointed out being a small country; the majority of businesses in New Zealand have less than twenty people which have difficulties implementing segregation of duties. **20%** of the interviewed participants mentioned that the lack of legislations, standards, and compliances in New Zealand also have impact on immature strategies within the organizations. Furthermore, **40%** of the participants commented that immature strategies expose four categories of vulnerabilities which can be exploited by prospective social engineers.

Thirdly, the social engineering-based attack examples given by the participants show the diversity and complexity of this form of attack. As they stressed, there is a need for multifaceted defence approach to mitigate the risks associated with social engineering. In agreement with the approaches identified in the literature, the participants suggested that education, appropriate technical controls, and security-enhanced products should also be adopted.

VII. Research Contribution, Limitations and Future Research

This study makes three contributions:

Firstly, it provides insights regarding the social engineering phenomenon from both theoretical and practical perspective and developing a conceptual model to demonstrate the findings.

Secondly, it enhances understanding of social engineering in terms of the impact of this form of attack to businesses and individuals, through illustration of real New Zealand examples from the research participants.

Thirdly, it provides a multifaceted defence approach towards mitigating the risks associated with social engineering.

The research limitations are twofold. The first limitation is the selection of the interview participants. The participants of this research were the IT practitioners in New Zealand who either had a security background or had an interest in security issues. As a result, there is a lack of understanding from the non-IT perspective as people's perception of the problem might be different. This can be justified as the purpose of this research is to collect insightful opinions about major issues regarding social engineering-based attacks in New Zealand. Therefore, it was not the researchers' interest to investigate the research topic from a non-IT perspective. Secondly, this study constructed a conceptual model for social engineering-based attacks based on the findings from the literature review and interview analysis with twenty-five New Zealand-based IT experts. However, the model and the underlying theory require further validations.

Opportunities for future research on the basis of this research are in three areas. First, as mentioned in the previous section, one area would be to validate the constructed concept of social engineering-based attacks by assessing the underlying theory of each identified entity. In addition to this, a more sophisticated model can be built using this conceptual model. Secondly, this research has provided detailed analysis of how to conduct social engineering attacks. The analysis can be used as the basic guideline to design an educational software application that educates people on how to act in different attack situations. Lastly, as part of this research, a multi-faceted countermeasure against social engineering-based attacks was illustrated. Each of the proposed defense approach can be seen as a future research direction.

References

[1] Twitchell, D. P. "Social engineering in information assurance curricula," in: *Proceedings of the 3rd annual conference on Information security curriculum development*, ACM, Kennesaw, Georgia, 2006.

[2] Granger, S. "Social Engineering Reloaded," 2006.

[3] Hinson, G. "Social Engineering Techniques, Risks, and Controls," *EDPACS: The EDP Audit, Control & Security Newsletter* (37:4/5) 2008, pp 32-46.
[4] DeWalt, D. "Cybercrime: The Next Wave."
[5] Keize, G. "Old worm makes comeback," Computerworld, 2009.
[6] McAfee "McAfee Advert Labs - Top 10 Threat Prediction for 2008," McAfee.
[7] McMillan, R. "Making a PBX 'botnet' out of Skype or Google Voice?," IDG News Services, 2009.
[8] Fu, R. Social Engineering-Based Attacks - Model and New Zealand Perspective, Master Thesis, The University of Auckland, 2009.