Managing Social Engineering Attacks- Considering Human Factors and Security Investment

R. Alavi[1], S. Islam[1], H. Mouratidis[2] and S. Lee[1]

[1]School of Architecture, Engineering and Computing, University of East London,
[2]School of Computing, Engineering and Mathematics, University of Brighton
e-mail: {reza, shareeful, s.w.lee}@uel.ac.uk; H.Mouratidis@brighton.ac.uk

Abstract

Soliciting and managing the protection of information assets has become a objective of paramount importance in an organizational context. Information Security Management System (ISMS) has the unique role of ensuring that adequate and appropriate security tools are in place in order to protect information assets. Security is always seen in three dimensions of technology, organization, and people. Undoubtedly, the socio-technical challenges have proven to be the most difficult ones to tackle. Social Engineering Attacks (SEAs) are a socio-technical challenge and considerably increase security risks by seeking access to information assets by exploiting the vulnerabilities in organizations as they target human frailties. Dealing effectively and adequately with SEAs requires practical security benchmarking together with control mechanism tools, which in turn requires investment to support security and ultimately organizational goals. This paper contributes in this area. In particular, the paper proposes a language for managing SEAs using several concepts such as actor, risks, goals, security investment and vulnerabilities. The language supports in-depth investigation of human factors as one of the main causes of SEAs. It also assists in the selection of appropriate mechanisms considering security investment to mitigate risks. Finally, the paper uses a real incident in a financial institution to demonstrate the applicability of the approach.

Keywords

Social Engineering Attacks (SEAs), Human Factors, Security Investment (SI), Security incident, Return on Information Security Investment (ROISI).

1. Introduction

Providing a strong security posture is crucial for business continuity. Currently with great threats of cyber attacks and virtual terrorism, security must be given adequate consideration. If they are not, everyday organizational activities will be grounded with real possibilities of loss, punitive financial fines and damaged reputation. SEAs undermine organizations' efforts to deal with security in an effective way. There are several malicious practices such as Advanced Persistent Attack that create security breaches in organizations (Siponen et al. 2010). Janczewski and Fu (2010) defined the SEAs with two distinct methods; the "Human-Based and Technology-Based" attacks. However, the role of people and certain human factors are contributing greatly to SEAs. The attackers crack the security of an information system by exploitation of human weaknesses. SEAs increase risks of financial loss, legal fees and reputational loss for organizations. It is a challenging task for organizations to deal with SEAs because they are human-oriented activities and human factors are difficult to deal with. This paper contributes to the link between the main human factors, which have been identified in previous study (Alavi et al. 2013) and SEAs with consideration of security investment. In particular, the paper proposes a language to analyze the attacks caused by human factors. This paper has adopted the Secure Tropos methodology to identify and analyze security concepts and extend it with these human factors and Security Investment (SI) so that appropriate justification can be taken into consideration in preventing such attacks (Mouratidis and Giorgini, 2004). Finally, the study considers a case study from a real security incident to demonstrate the applicability of the approach.

2. Related Works

There have been a number of works that focus on analyzing SEA attacks. This section includes the works that are relevant to the study's approach. Janczewski & Fu (2010) provided a conceptual model in order to understand SEAs impacts on individuals and businesses and present a defensive approach to mitigate these risks. The study focused on IT departments and a more abstract view of SEAs without considering SEAs concepts related to human factors and their relationships to the concept of SI. Greitzer et al (2014) looked at the insider threat that derives from SEAs. The study considered some related human factors but concentrated mainly on unintentional insider threats whilst observing psychological and social characteristic of people. Karpati et al (2012) used a comparison study between mal-activity diagram and misuse cases and presented two modeling techniques. This study attempted to provide a conceptual comparison in order to find the advantages and efficiency of each approach. It provided three main concepts; risk, asset-related and risk-treatment concepts. Although the paper concentrated on SEAs and provided a concrete discussion in the validity of the study, it did not embrace SI and actors such as human and security systems. In addition, the paper distinguished between information security assets and business assets, which can potentially be a confusing issue when it comes to SI. Some other studies concentrated on specific attacks such as phishing attacks (Finn & Jakobsson 2005) or advanced persistent attacks (Shakarian et al 2013).

All the above-mentioned works contribute towards investigating SEAs. However, none of these works explicitly focus on human factors, which are one of the main reasons for SEAs. In particular, SEAs require a systematic approach to analyze the complex human factors and solutions in order to address any issues relating to them. Security markets are dominated with technical solutions promising much in security efficiency whilst brushing aside human elements despite overwhelming evidence to the contrary. This work contributes in analyzing human factors and proposes solutions and security investment in these solutions so that an organization can make the right decision relating to information security.

3. Social Engineering

3.1. Social Engineering Attack

Social engineering is the act of manipulating a person to take an action that may or may not be in the target's best interest which include obtaining information, gaining access or getting the target to take a certain action (Hadnagy and Wilson, 2010). Responding to the threats of SEAs using technological resources and tools would not be enough to deal with the associated risks because people are at the centre of such attacks and they play a vital role in it. Organizations may use various tools such as web server security to detect and minimize SEAs but they have difficulty in preventing and responding to human actions and behavior in socially engineered incidences. SEAs resulted mainly in the exploitation of many related issues of human factors. There are specific factors, which were identified, in the previous study and play important roles in such attacks (Alavi et al., 2013): Lack of awareness and ample set of skills, inadequate communication skills, Lack of supervision and sufficient involvement of management. Therefore, it can be concluded that human factors and human social interactions can be engineered for exploitation in gaining access to an organization's assets. The lack of, or an inadequate control mechanism leaves human factors open to exploitation. Attackers generally use different deceptive methods to exploit users who have a lack of awareness about the system and its surrounding context.

3.2. Reasons for Social Engineering Attacks

Human factors remain essential to any SEAs because no matter how many training programs or control mechanisms are deployed; people are the weakest link in security (Hadnagy 2011). SEAs can cause a great deal of disruption to everyday business activities and create financial, social and technical mayhem in which the impacts may go beyond geographical borders and organizational boundaries. Therefore, dealing with SEAs would be in the best interest of any organization. According to the (Verizon 2014) report, human factors are the main sources of SEAs. People can be easily socially engineered which leads to compromise of information systems in organizations. Even when attackers use complex and sophisticated technical hacking methods they would consider using people as a main tool in delivering their malicious software. For example they use e-mail attachments, which can easily mislead people and deliver the payloads of malicious program in order to gain access to a system. This type of attack is just one example out of hundreds of methods, which has worked both with big organizations and central governments. Janczewski and Fu (2010) identified five main causes of SEAs, i.e., people, lack of security awareness, psychological weaknesses, technology, and defenses and attack methods.

3.3. Social Engineering Attacks Taxonomies

There are certain concepts which must be considered to provide adequate defense mechanism against SEAs either detective or preventive. These include the style of attacks with consideration of human factors, the expected result of attacks and the possible impacts. This study developed SEA taxonomy in order to identify the main concepts and their attributes of the proposed language. Figure 1 shows how an attacker can plan an attack, which has variable impacts such as disclosure of data and theft of resources. The impact/s fulfils the goals and objectives of the attacker whether financial, personal, or political gain.

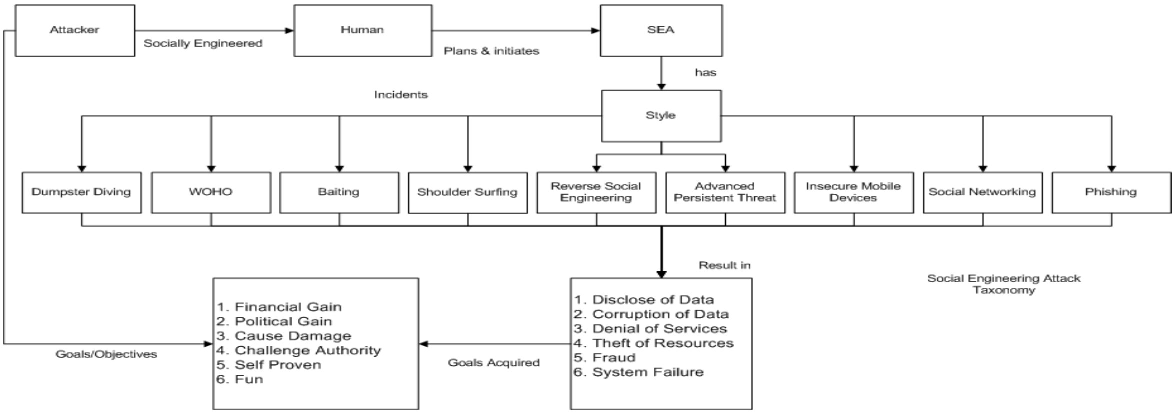

Figure 1: Social Engineering Attack Taxonomy

4. Language for Managing Social Engineering Attacks

4.1. Framing concepts

The process of securing information has become more critical than ever. When security is mission-critical and tied to revenue chains and compliance, then it has significant bottom-line impact. Security, cannot tolerate any performance delays by protection mechanisms, and require extra attention to ensure its success and at the lowest possible cost. Most research has concentrated on the success of security without consideration to cost that has an impact on the overall Return on Information Security Investment (ROISI). However, both security concepts of ISMS process and cost concepts of ROISI process have the same goal which includes the protection of information assets to prevent extra cost as a result of financial and reputational losses. Adopting a combined framework would enable us to address both security and investment concepts. The novelty of this work is a language that combines the concepts from security, risks and investment to support defense mechanism against SEAs and to assist in the calculation of return of SI considering human factors. The paper adopted Security Tropos to analyze security concepts such as actor, security goal, vulnerability, threat and plan and extended it with risks and SI from which ROISI can then be appropriately calculated in future study (Mouratidis and Giorgini, 2004). These concepts equip security architecture to establish the security-investment relationship and the systematically reasoning of them. This section lays out an overview of the concepts used in the Metamodel.

Actor: is the central concept of the proposed language. It represents an entity that has strategic goals and intentions within a system and organizational settings. An actor in this case can be human or the ISMS. In particular, human actor includes several factors such as awareness, communication and the involvement of management. ISMS actor has properties such as security policy and physical security.

Goal: is a stakeholder (Actor) objective or strategic interest for a system and its surrounding environment. The strategic objective of actor is to achieve goal and does not care how it is achieved but goal satisfaction should be formulated in agreement of shared development amongst all actors. The proposed language differentiates between security and organizational goals. Organizational goals represent goals that are important at an organizational level. Such goals include profitability, compliance, continuity, reputation and performance. Security goals support security needs. This means a secure goal serves actors' and concerns associated with goal (Giorgini et al, 2006). Confidentiality, integrity, availability, auditability and authenticity are the security goals. An adequate security balance can be obtained by exchanging security requirements and other functional/non-functional requirements of the security system that is equipped according to the goal.

Risk: Risk is the potential damage of consequence of a security incident. The incident arises from information process in organizations that may be maliciously exploited. SEA is an example of such exploitation. Risk is present in every aspect of information process and poses a possible loss within an organization. The proposed language has three different types of risks including; **financial loss**: A risk, which is difficult to quantify. However, this risk can be a direct loss of financial accounts or a loss as a result of disruption of business. **Legal fines:** A risk of organizations in receiving a fine as result of a security incident which violates legal obligations. **Reputational loss**: This is a risk, which traditionally was a result of reporting to the regulator. The risk of reputational loss could be the loss of attracting new customers and in some cases could affect credit rating.

Security incident: In the proposed language SEAs create threats that are caused by actors using different types (Figure 1). The possible threats can be: Internal system compromise, stolen customer data, phony transaction, insider attack and DoS attacks.

Vulnerabilities: A weakness in ISMS procedures, design, implementation, or internal controls that could be exercised and result in a security breach. Despite being patched by control mechanism a system always has vulnerabilities. This concept can be addressed by the vulnerability assessment which provides guidelines for protection mechanism. It consists of defining and classifying system resources, assigning levels of importance to the resources, identifying potential threats to each individual resource, developing countermeasure strategy and implementing methods to minimize the consequences of SEAs.

Security investment (SI): the concept of SI is defined as the capital that is being made available for security solutions via protection mechanism in supporting a goal. SI in this case is not a direct measure of the profit but prevents or at least, lessens the loss that could occur from human related security incidents. Therefore SI should consider technical and non-technical cost implications. The reason for this is that the cost of preventive measures of SEAs is varied whilst the landscape of threats and consequently the risks are changing. At the same time other attributes require attention. They can be business impact analysis (BIA), threat description, vulnerability assessment, risk evaluation and treatment.

Plan: is a workable long-term (strategic) mid-term (tactical) and short-term (operational), actions for reasoning and achieving goal must be utilized and adoptable for actors. Protect mechanism requires a plan to achieve ISMS security and organizational goals by ensuring strategic security and SI improvements. Long-term strategy entails issues related to human factors portfolio (involvement of senior management) and risk analysis. Mid-term (tactical) plan also concerns a human factors portfolio (awareness and communication) and tactical improvements such as maintenance and communication. The short-term (operational) phase of the plan is about allocation of critical IT assets, human factors portfolio and security implementation practice.

Protect mechanism: is the real control for addressing strategy and supporting plan. It can be detective or preventive for SEAs. It also protects information assets and assists patch system vulnerabilities. They can be either technical or non-technical and are listed as part of SI.

The goal, actor and plan used and defined is based on the entities of Secure Tropos. The security-risk language and other related concepts are adopted from ISMS principles whilst SEA incidents are defined based on wider SE concepts. The SI relies on ROISI process that was briefly explained earlier and will be followed by future study. Figure 2 presents the Metamodel, which is the combination of the above concepts, linked with some of the Secure Tropos security concepts.

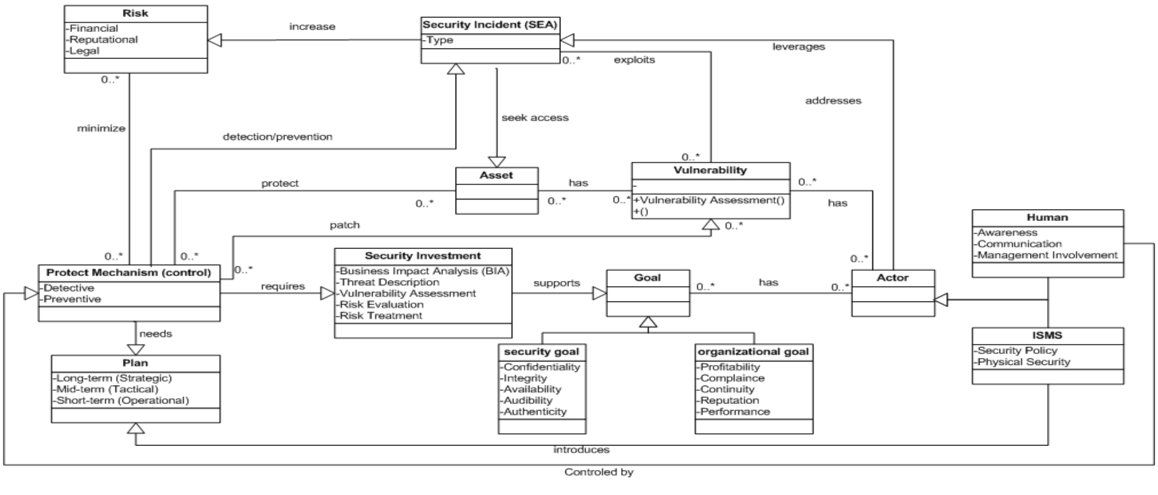

Figure 2: Proposed Metamodel

This paper approaches the concepts of security incidents, SI and humans as actor all play a major role whilst the protect mechanism is the core concept. Protect mechanism relies on strategic planning in providing detective and preventive methods for security incidents. It assists patching vulnerabilities and assets protection, which are mainly information (soft) assets. Once SI is configured, then detective and preventive control mechanism could potentially mitigate financial, reputational and legal risks. The mid and long-term plan strategy also supports protect mechanism in addressing awareness, communication and management support of actor (human) entities. Actor has vulnerabilities which can be exploited and influence security incidents. The identified detective and preventive controls create a set of consequences in the system. The consequences require validating against security incidents and SI to establish the leverage of the incident and actor in the system. If this is not justified then protect mechanism must be equipped to replace the gap requirements of planning and investment.

5. Case study

To demonstrate the applicability of the proposed approach, the paper deployed the proposed language through a case study scenario. The following description is a real and successful SEA incident that happened in a financial institution within the UK. This incident was an isolated but, successful case and the organization did not publicize it. One of the authors of this study had access to the incident log and therefore the company's name cannot be revealed.

Scenario

An employee received an email from one of the managers' referencing an invoice hosted on a cloud file sharing service. A few minutes later, the same employee received a phone call from another manager within the organization, instructing her to examine and process the invoice. However, the invoice was a fake and the manager who called the employee was an attacker. The apparent invoice was in fact a Remote Access Trojan (RAT) that was designed to contact and command-and-control (C&C) the server. By using the RAT, the attacker took control of the employee's computer instantly. The attacker managed to breach a part of the server as the multi-layered encrypted server prevented him from getting access to all the servers. This attacker used a socially engineered attack for financial gain. Before the attack was stopped they succeeded in getting a financial incentive in the region of £50,000.00.

***Actors**:* The main actors involved in the scenario are:

- **Employee**: The employee here is the target victim. She was exposed with malicious pretexting and an identity theft by the attacker. She was a victim of a malicious and successful pretexting method.
- **Employee Manager**: The scenario also includes a victim target whom was a manager as an employee of the organization. The manager was a victim of impersonation. The attacker used the victim's defined organizational authority.
- **Attacker**: The attacker was an ex-contractor who previously carried out some network maintenance and had some insider knowledge from the target

company. However, the attacker needed to elicit his knowledge so he used various sources such as, the organization's web site and social media for this purpose. The attacker implemented some SE techniques in order to be confident enough to run the attack. He exploited various weaknesses of the target victims, such as lack of authentication in the communication process and the skill of the target employee. The attacker manipulated the employee to behave in certain ways in order that the attacker accomplished his goal, which was to access financial data for financial gain.

- **ISMS**: is a target system and provides security policy and physical security to ensure security is sound. The nature of this attack reveals that an employee is easily tricked. Something which security policy should re-adjust itself to. The re-training program lacks adequate phone calls and E-mail authentications' procedures.

Goals: The following goals have been observed:

- **Financial gain**: The attacker's goal is to obtain financial information in order to gain financial reward.
- **Perform duty**: The victim employee's goal is to perform their duty and follow the ISMS practice of the organization. In addition, the target victim employee's desire is to protect her employment contract that can be in line for review because it has been breached.
- **Organization goal**: the victim target organization requires continuity, performance and profitability needs to be maintained whilst the reputation and its compliance objectives are preserved.

Security Incident: The incident was mainly exploited by a phishing attack in which the attacker impersonated one of the managers. The main reason the attack was successful was because the employee followed the existing ISMS practice but the authentication process was not adequate in identification checks over the phone.

Vulnerabilities: The attacker mostly followed different elicitation methods to consolidate information before making the attack. The main weakness was the lack of an authorization mechanism for phone call verification.

Risk: The incident posed several possible risks in context.

- Financial loss: Attacker successfully obtained financial gain which is estimated at £50,000.00,
- Classified data leakage: There was a specific data related invoice that helped the attacker exploit the attack. This means that there was a violation of the Data Protection Act by the organization.

Plan: In this scenario the lack of improvements in the three stages of planning including long, medium and short-term is clear. The human factors portfolio raises major concerns whilst some technical improvements in authentication of communication seems necessary.

Protect mechanism**:** The study observed following protection mechanism for mitigating root causes of the incident so that the chance of success of such attacks can be minimized in future. Therefore, if the control mechanism was adequate enough to detect socially engineered activities then the attack could have been detected and dealt with adequately. This could have been done through a detailed training program as a soft control measure. A hard (technical) measure could have been established for the authentication of phone communication where such requests in accessing sensitive data require a password. This helps to establish an authenticated communication channel. This mechanism requires investment in updating security policy and providing new training reminders that seeks management support. Because the attacker was an ex-contractor, a review of access control measures is required to ensure unauthorized access is denied to the use of out dated credentials.

Security Investment (SI): intends to identify the investment that organizations require in order to deal with all security incidents effectively and adequately. The following questions could help in reaching the right decision of the executive management team: What obligations is the organization bound by in terms of compliance? What sanctions in information management in this scenario have been hit? Does the organization feel over-retention is a concern or is a necessary price to pay for compliance? Future study should look at the quantification of ROISI to response to the above questions. As far as this study is concerned, investment could more than cover the loss involved in an incident and is the main part of the proposed language. For the purpose of this study, the paper introduced the preliminary expected cost to cover the loss arising from incidents from the following parameters: External Services Cost ES(C), Purchasing Cost P(C), Employee Cost E(C), Administrative Cost A(C), Legal Costs L(C). Therefore the total expected cost of new and updating control mechanism would be: TEC(T) =ES(C) + P(C) + E(C) + A(C) + L(C). Future study should look at other parameters of investment concepts such as, Single Expected Attack Loss, Insurance Claim, Revenue Loss (from existing/potential clients) and Average Margin.

6. Discussion

The paper presents a SEAs risks-based language considering human factors and security investment. It includes several concepts such as goal, actor, SI, incident, risk, and protection mechanism that allow the analysis of SEA incidents and proposes appropriate control in a structured manner. The main reason for the discussed incident was because of the way in which employees were deceived with infected E-mail and hoax phone calls. This timely work contributes in addressing the challenge of managing human factors and security investment, so that possible risks can be mitigated. The study demonstrates the concepts through case study. This paper’s observation is that the organization’s current protection mechanism lack consistency. There are two important issues that have not been considered. Firstly there is the nature of attacks in which employees are easily tricked. Secondly that controls are needed by the application of patching. Employees are required to be trained in dealing with email and phone authentication processes, to distinguish between genuine and invalid hoax communications. Without knowing how much organizations would get in return from extra and new investment, it is a little like walking blind folded along a path. The concepts of language support analyzing the factors with realistic proposed solutions to control SEA based on SI. CISOs in organizations are the main beneficiary of this language in addressing security policy and security related human factors. There are certain limitations in this study. However the most important consideration is the nature of a business as well as the differences in organizational, culture and risk appetite.

7. Conclusions

With the rapid grown of information technology and the subsequent rise of an information society, the cost of information security and consequently the return of any investments in this area become one of the major concerns of organizations and governments. The objective of this work is to present a language that provides an understanding in the relationship between various concepts involved in SEA incidents considering human factors. These concepts systematically support analyzing SEAs and identifying appropriate mechanisms and investment for a mechanism to protect SEAs. The study then illustrated the use of this language in a real-life circumstance within a case study. The ROISI process which will be developed in future study will provide a valuation of annual expectancy in loss and SI. To develop a model from this language further research is required.

8. References

Alavi, R., Islam, S., Jahankhani, H. & Al-Nemrat, A. 2013. Analyzing Human Factors for an Effective Information Security Management System. International Journal Of Secure Software Engineering (IJSSE) 4, 50-75.

Alavi, R., Islam, S., Mouratidis, H. 2014. A Conceptual Framework to Analyze Human Factors of Information Security Management System (ISMS) in Organizations. Human Aspects of Information Security, Privacy, and Trust. T. Tryfonas and I. Askoxylakis, Springer International Publishing. 8533: 297-305.

Hadnagy, C. 2011. Social Engineering: The Art of Human Hacking. Indianapolis, Wiley Publishing Inc.

Hadnagy, C. & Wilson, P. 2010. Social Engineering: The Art of Human Hacking, Wiley.

Janczewski, L. & Fu, L. 2010. Social Engineering-Based attacks: Model and New Zealand Perspective. Computer Science and Information Technology, 847-853.

Mouratidis, H., Giorgini, P. 2004. Enhancing Secure Tropos to Effectively Deal with Security Requirements in the Development of Multiagent Systems. 1st International Workshop on Safety and Security in Multiagent Systems. N.Y. USA.

Verizon Enterprise Solutions. 2014. 2014 Data Breach Investigations Report (DBIR). Available: http://www.verizonenterprise.com/DBIR/2014/ [Accessed 01/10/2014].

Siponen, M., Pahnila, S. & Mahmood, M. A. 2010. Compliance with Information Security Policies: An Empirical Investigation. Computer, 43, 64-71.

Finn, P. and Jakobsson, M. 2005. Designing and conducting phishing experiments. IEEE Technology and Society Magazine, Special Issue on Usability and Security.

Shakarian, P., Shakarian, J., & Ruef, A. 2013. Introduction to cyber-warfare: A multidisciplinary approach. Maryland Heights: Syngress Publishing.

Greitzer, F. L., Strozer, J. R., Cohen, S., Moore, A. P., Mundie, D. & Cowley, J. Analysis of Unintentional Insider Threats Deriving from Social Engineering Exploits. Security and Privacy Workshops (SPW), 2014 IEEE, 17-18 May 2014. 236-250.

Karpati, P., Sindre, G., S. & Matulevicius, R. 2012. Comparing Misuse Case and Mal-Activity Diagrams for Modelling Social Engineering Attacks. International Journal of Secure Software Engineering (IJSSE), 3, 54-73.