2017

Tonga’s organisational vulnerability to social engineering

Raymond Lutui
Auckland University of Technology

Viliami Fe’aomoeata
Christ’s University in Pacific

DOI: 10.4225/75/5a84f20d95b49
Lutui, R., & Fe’aomoeata, V. (2017). Tonga’s organisational vulnerability to social engineering. In Valli, C. (Ed.). (2017). The Proceedings of 15th Australian Information Security Management Conference, 5-6 December, 2017, Edith Cowan University, Perth, Western Australia. (pp. 33-41).

TONGA'S ORGANISATIONAL VULNERABILITY TO SOCIAL ENGINEERING

Raymond Lutui[1], Viliami Fe'aomoeata[2]
[1]Digital Forensic Research Laboratories, Auckland University of Technology, Auckland, New Zealand
[2]CUP Research Institute, Christ's University in Pacific, Nuku'alofa, Tonga
rlutui@aut.ac.nz, vfeaomoeata@gmail.com

Abstract

Tonga is a small developing island in the south pacific and ICT is still in its early stages. In this paper we ask the questions, what is social engineering and who is this social engineer, what are the threats to Tonga, how can these threats be identified and which countermeasures can be taken to mitigate the risk of social engineering? The answers to these questions will lead to a social engineering risk management framework to make the risks of social engineering more transparent and help organisations implement mitigating controls against social engineering. The study was performed in four chosen organisations in Tonga, who were involved with Information Communications, Finance, and Cyber Security in order to model threats and countermeasures and develop a risk management framework.

Keywords: Risk management; Social engineering; Information security; Cyber security; Organisational Vulnerability; Security threats; Threat assessments.

INTRODUCTION

The technical aspects of information security have been in the spotlight for several years (Solomon and Chapple, 2005, p.56), and has made much progress. In general, large improvements in security can no longer be attained by upgrades in hardware or software. It is therefore difficult for attackers to achieve their goal through technical attacks alone and their focus shifts (even more) to the organisations employees (Richards, 2008, p.41). As a result, organisations need to direct increased attention toward the undertreated human factor of information security to guard and stay in control of their critical information. For many organisations, the weakest link in information security is now human (Mahfuth et al., 2017, p.1). Organisations need to raise the security on this human factor to an even par with the technical security Legg et al., 2015, p.1). In response, information risk management the top training priority for Information Technology security professionals (Luiijf, 2012, p.57). Organisations are looking to develop flexible frameworks that give insight to the risks involved and help them adapt to changing environmental factors.

Although there have been studies conducted on the human factor of Information Technology, it is still a relatively unexplored field of scientific research. In most cases, the literature does not have a scientific foundation and does not give a clear overview but merely discuss case descriptions (Tsohou et al., 2010, p.227). However, all of the previous mentioned studies show that the human factor can cause great damage to organisations, not only financial but, also to the organisation's image, which in turn influences the organisations goals and continuity in the long run (Drevin et al., 2006, p.448).

Ironically, employees are not only important assets, but also pose a great threat. Employees not only know where to look but have the advantage of obtained trust and accessibility to systems (Nurse et al., 2014, p.271). Attackers can misuse the employees or could even be one of them. There have been known cases of technical hack, and the most notorious human hacker, Chris Hadnagy, asserts that breaches start with a phishing email or vishing call, then they go to a technical hack (Shin, 2017, p.1). This study will primarily focus on the threats from external parties, however, also internal threats and culminate in a high level social engineering risk management model. This can be used to gain transparency on the subject, implement mitigating controls, and help organisations manage their social engineering risks.

This study focuses on '*social engineering*', the manipulated compromise. Mitigating the threats of this manipulation will also reduce the intentional and unintentional compromising of systems and information therefore, lower overall risk. While this research hopes to provide incentives that may help to ensure business continuity and give organisations in Tonga a clear view on social engineering, it also aims at finding out how to strengthen the weak link in information security, the human factor, by looking at:

"How social engineering occurs in organisations?"

The measures that can be used to stop social engineering from causing harm. How an organisation can measure the risks and their protection from social engineering threats and if necessary apply appropriate countermeasures to mitigate these risks and stay in control of their information, thus ensuring business continuity.

LITERATURE ANALYSIS

Social engineering has been defined as the unauthorised acquisition of sensitive information or inappropriate access privileges by a potential threat source, based upon the building of an inappropriate trust relationship with a legitimate user (Dudek, 2006, p.1). That is, pretending to be someone you are not, with the goal of misleading someone into giving out information they should not give. Social engineering is an aspect that involves both intellect and technical experience, but more importantly it is an evolving phenomenon that needs to be monitored constantly. If attackers are willing to be consistent in finding loopholes in the system, then security experts should balance and overcome that attempt. With that thought in mind, the basis of this literature analysis is to find out what is trending in not only the cyber world, but also to assess the status of organisations in Tonga with regards to social engineering security.

As a result, it is evident in the literature that a number of researchers have invested time and resources into exploring social engineering. In addition, they look for the latest techniques. However, despite the vastness of the exploration, this analysis will focus on a certain number of key elements that relates to the area of interest.

Hackers and Social Engineers

Hacking and social engineering are closely related. Social engineering tactics are applied to gather information in preparation of a hack and the motives and goals of both types of attacker are related (Ziccardi, 2013, p.75), as social engineers are also known as '*people hackers*'. It is therefore important to know who these (people) hackers are (Warren, & Leitch, 2010, p.427). In this section, a description of hacking and the hacker will be given along with the motives a social engineer may have.

Hackers, Crackers and Phreakers

There are hackers with good intentions. For instance, searching for vulnerabilities in the information system so they can be controlled. There are also hackers with bad intentions, using the identified vulnerabilities for personal gain. There are three types that all get the predicate 'hacker' in the media; hackers, crackers and phreakers (Milberry, 2012, p.112). The jargon dictionary defines a hacker as: "A person who enjoys exploring the details of programmable systems and how to stretch their capabilities, as opposed to most users, who prefer to learn only the minimum necessary" and "one who enjoys the intellectual challenge of creatively overcoming or circumventing limitations" (Watson, 2012, p.260). A hacker is therefore someone who seeks challenges and overcomes boundaries using his or her skills. Hackers follow an ethical code and do not act illegally, which differentiates them from the crackers (Long & Wiles, 2008, p.104)

A cracker is someone who breaks into the system with the goal of theft or vandalism and therefore does not act ethically (Rahalkar, 2016, p.90). Crackers form small groups within the hacking community and are seen as 'a lower form of life' by other hackers (Voiskounsky and Smyslova, 2003, p.178). Another name for these crackers is 'dark-side hackers' (Svensson, 2016, p.90). Finally, phreakers use information and social engineering skills to break into telephone systems and use these for various purposes such as, making long distance phone calls at another's expense, stealing phone card numbers or pretending to call from a secure location. People hackers - in contrast to technical hackers - focus on the weaknesses in the human, instead of the technology they use. The people hackers referred to in this study all have malicious intent and could therefore be classified as 'people crackers' according to previous classification (Barghuthi & Said, 2014, p.2). For the purposes of this paper, the term hacker will imply to those hackers, or crackers working with malicious intent (Richards, 2008, p.40).

SOCIAL ENGINEERING ATTACKS

Knowing why social engineers might attack is crucial for estimating the likelihood of a social engineering assault on a specific organisation, and to implement appropriate measures and controls to counter this assault (Lafrance, 2004, p.12). The motivation of different subcultures within the hacking community will now be discussed

followed by the motives of the social engineers. Bodhani (2013) identifies four subcultures within the hacker community, each with different motivation; casual hackers, political hackers, organised crime, and internal agents (p.65). There are also hackers that do not act as a member of a subculture. The Australian government performed research on the personal motives of a hacker (Madarie, 2017, p.80) such as monetary gain, intellectual challenge, power, and so on. The motives of the social engineer can be classified according to a variation on the results of this research (Krone, 2005, p.2). For each category, a general description of the motive is given, a classification in malicious or good intentions, and what role social engineering can play in an attack with this motive.
The way social engineering can be used in an attack is subject to the goal of the attack. If the goal is to acquire specific information, social engineering can play a great part in the attack. But the main challenges taken up by attackers are still technical; in most cases therefore social engineering will be used to gather information and prepare for the final attack. To stop the social engineer from succeeding, organisations need to apply measures to counter the social engineering attacks and tactics. They can change the environment of the asset, they can choose to act on occurring attacks or they can mitigate the social engineering risk by the structured implementation of countermeasures (Smith et al., 2013, p.250). This study focuses on transparency of social engineering and therefore on the structured implementation of countermeasures. Also, the information security controls, which encapsulate several measures to mitigate the social engineering risk will be classified and listed. After which the key elements pertaining to the human factor are discussed in more detail.

Information Security Controls

In order to secure organisation's data, certain controls must be in place. There are several proposed classifications found in the literature however, Harnesk & Lindström (2012) defines the three most cited dimensions - confidentiality, integrity and availability (CIA) (p.80). *Kind of measure*; physical, logical or organisational. *Moment of action*; corrective, repressive, preventive and detective. Most other models do not classify the reason of protection because, social engineering threatens the confidentiality, integrity and availability and the applied controls need to protect against all of these (Luiijf, 2012, p.56). The classification is based in part on a classification by the National Institute of Standards and Technology (NIST) and complemented with input from the IT Infrastructure Library (ITIL), they both classify the controls on two dimensions. The classification proposed here also consists of two axes, the first according to the *function of control*, the second according to the *level in the organisation* (Dempsey et al., 2011, p.5).

Function of Control

The function of a control is related to its place and effect in the security management process. (Tse, 2004, p.1507). The ITIL classification for security management is used to complement and add an extra level to the process (McPhee, 2008, p.5), defined by the NIST as this only discusses a limited number of functions. Security controls are safeguards or countermeasures employed in order to avoid, detect, or minimise security threats or risks to information, computer systems, or other assets (Tayouri, 2015, p.1098). These controls can be classified based on several criteria. For instance, the time they act, in relation to a security incident: Before the event, ***preventive controls*** are employed to prevent security incident from occurring such as, locking out unauthorized intruders; if a security incident occurs; during the event, ***detective controls*** are intended to identify and characterize an incident in progress such as, by sending out an alert; after the event, ***corrective controls*** are in place to limit the extent of any damage caused by the incident e.g. by recovering the organisation to normal working status as efficiently as possible (Whitman, 2004, p.52). To support the specific controls against social engineering some *general security controls* need to be implemented. These form a base for the more specific controls and will probably -in part- be implemented already to protect other assets from other forms of attack.

DESIGN OF THE STUDY

A guidance of a methodology is highly recommended to maintain the integrity of the findings. Information security experts are aware of social-engineering threat but to date have never seemed to focus their efforts on studying and understanding in depth how and why cyber criminals are using social-engineering method as a weapon (Alexander, 2016, p.2). Yildiz (2007) argued that, some research suffers from definitional vagueness of its concept (p.647). A researcher has to decide the type of research to be conducted in order to answer the pivotal research question that will disclose new knowledge. Exploratory research, on the other hand, is employed in this type of study as it allows the researcher to gain a deeper understanding of an issue or problem (Straub, et al., 2004, p.63).

Due to the fact that this topic has not been explored in depth and never in Tonga, Exploratory Research approach is employed to guide this study. An exploratory study is a valuable means of finding out 'what is happening; to seek new insights; to ask questions and to assess phenomena in a new light (Saunders et al., 2012, p.139). Exploratory research design does not aim to provide the final and conclusive answers to the research questions, but merely explores the research topic with varying levels of depth but to help to give a better understanding of the problem (Singh, 2007, p.38). Unstructured interviews are the most popular primary data collection method with exploratory research (Sreejesh, et al., 2014, p.47). The interviews were held using a leading questionnaire of open questions. The questionnaire consists of the following stages as represented in figure 2:

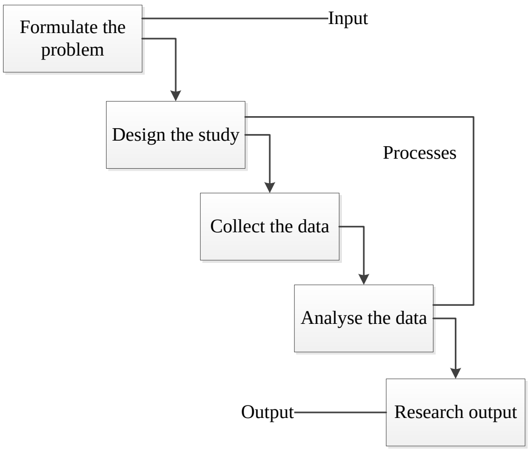

Figure 1: The design of the study

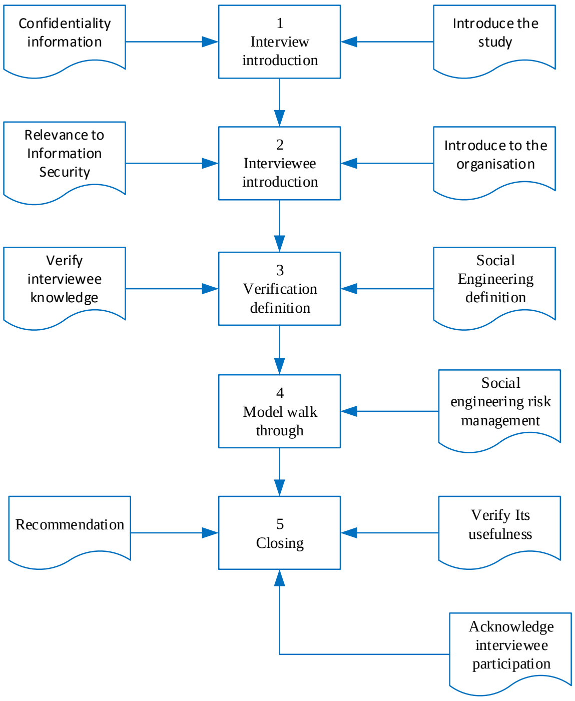
Confidentiality information
1 Interview introduction
Introduce the study
Relevance to Information Security
2 Interviewee introduction
Introduce to the organisation
Verify interviewee knowledge
3 Verification definition
Social Engineering definition
4 Model walk through
Social engineering risk management
Recommendation
5 Closing
Verify Its usefulness
Acknowledge interviewee participation

Figure 2: The questionnaire steps

The questionnaire structures the interview but still makes it possible to go deep enough to answer the research questions with a clear foundation.

Case Selection

The interviewed organisations were chosen based on the reliance of their business on information and IT and the level of risk of a social engineering attack. The interviews have therefore been held with an international IT service organisation due to its business focus on information processing and storage for external parties; a consulting organisation whose greatest assets are its personnel and knowledge; a regional governmental organisation due to its increased risk to a social engineering attack; and the Computer Emergency Response Team of the Tongan government (CERT) as the focus of this organisation is on the cyber security within the government by coordinating IT security incidents, informing and advising on these incidents and supporting the governmental organisations in the prevention of, and response to security incidents. All these organisations have a different perspective on information, its value, the risks they run and possible counter measures. Within the visited organisations the interviews where held with security officers and/or other security responsible personnel. Together these interviews represent a valuable perspective on social engineering as these organisations and specific interviewees should be the ones at the forefront of information protection from for example social engineering. Next to these interviews, the opportunity presented itself to discuss this matter during a cyber security seminar held at Tonga National Centre followed by discussion between the security representatives of several governmental organisations, as well as organisations from the private sector.

RESEARCH FINDINGS

The findings from the interviews have been de-identified and have only in part been related to the organisations or market. The confidential use of interview findings was a precondition for cooperation of the organisations as the provided information could be used in identifying participating organisations and vulnerabilities within these, which is not the intention of this research. Therefore, diagrams and organisational descriptions cannot be made any more detailed. The following findings are related to the organisations activities and are structured according to the stages of the questionnaire followed by relevant comments not directly related to the questionnaire.

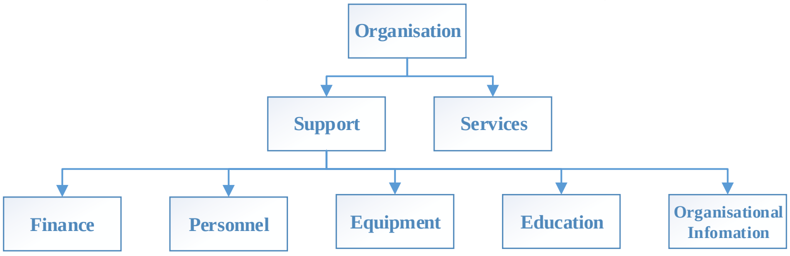

Figure 3: Organisation's activities

The organisation is divided in two parts, one executive in which the main activities are performed, the other supporting in which administrative activities are performed. The interview clearly focused on the organisational information division. The interview was held with the Chief Company bureau services, responsible for the organisational information.

Social engineering risk assessment model

The interviewee was not familiar with the term 'social engineering' but did recognise the description and examples. During the interview, the stated definition was used as reference.

Organisational Description

As the interview focused on the 'organisational information', the organisational description follows. The workplace and workstations are not related to the functions except for data mining. Access is not restricted to the local environment; however private use is restricted. Internet access is only available when necessary for the role or function an employee performs. The functions can be divided in three groups; primary, supporting and management. Authorisations are granted on a need to know basis and related to functional profiles. More authorizations may be provided on request. Segregation of duties is implemented within and between the functions.

Threat Identification

The organisation handles highly sensitive information, which is of great interest to criminal organisations as well as curious social engineers and hackers. But in general, all information in the organisation is of interest and can be of use to the social engineer. A short list of threats where identified, detailed threats more specific to the organisation have not been listed:

- Internal reports do not follow a workflow and can be anywhere on the work floor.
- Not all information is classified and can therefore be handled improperly.
- Access is logged. However, it happens that people log on to another's profile or use another's password.
- Some external parties need access to the system before they can be screened. However, these persons should be under supervision constantly.
- It is possible to intercept classified communications.
- People working at home create a threat.

Vulnerability Identification

Some vulnerability can be derived from the threats:

- It is not known where information is during processing; there is no accountability.
- Classification procedures are not followed.
- The password security policy is not followed.
- The authorisation process is not suitable for some activities.
- Some means of communication are not secure; however, they are necessary for operations.
- Procedures for media usage are not followed.
- People do not follow the information security procedures outside the office.

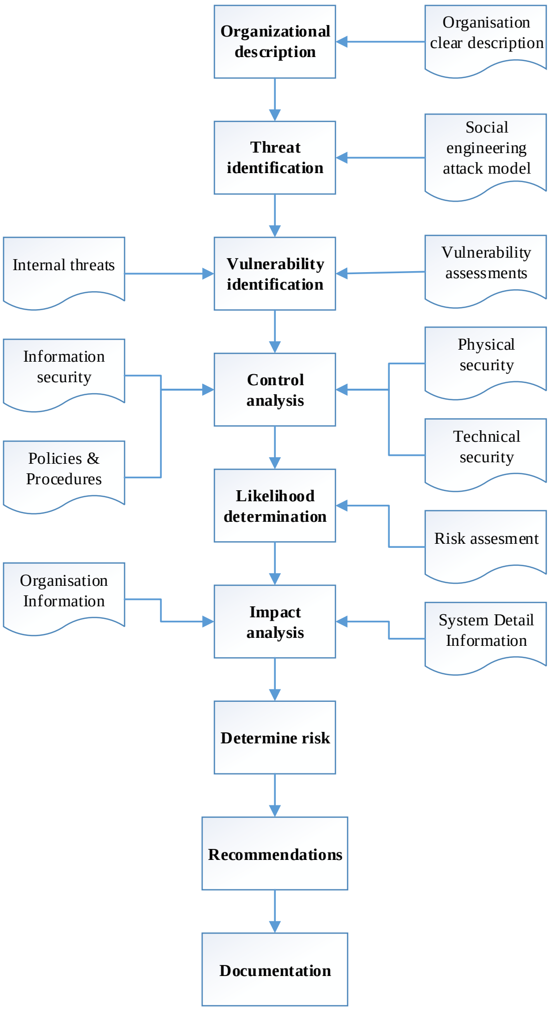

Figure 4: Social engineering risk assessment model

Prior to the interview, this organisation was faced with bad media coverage due to leakage of information after careless handling. The organisation thereafter performed a specific assessment on the information crossing the organisational boundary, this lead to the implementation of specific controls to counter this vulnerability.

Control Analysis

Some examples of controls are - Policy is implemented to stop information from crossing the organisational boundary. USB ports are generally disabled, Information that does need to leave the organisation on a memory stick or over the internet is secured through encryption, There is an awareness project that relates to the awareness of the information you use and training in how to use this so it stays secure, Leakage through personal contacts is traced and measures are taken if necessary, There are heavy penalties on deliberate leakage, Physical access is restricted through specific measures and the last one is, Penetration tests are performed, focusing on technical hacking through for example WIFI connections and Smartphones. But also, social engineering is tested through physical penetration testing and desk sniffing. The findings from this are used to confront people during the awareness trainings.

Likelihood Determination

There is a fair likelihood a social engineer can gather information from this organisation. However, more critical information will be less likely to leak due to the need to know basis on which it is spread through the organisation. In contrast, some threats on less critical information are simply accepted. So, the likelihood depends on the information and cannot be determined in general.

Impact Analysis

There are two general consequences of a successful social engineering attack;

- The image of the organisation can be harmed.
- The organisational processes and even people can be harmed.

Determine Risk

Even though awareness training and penetration tests are implemented there is still some social engineering risk. The organisational process sometimes prevails over the risk of leaking information. However, the risk is still present due to careless personnel.

Recommendations

Organisations need to follow a security management process consisting of a policy statement, followed by awareness, in turn followed by audits. In discussion with the interviewee, the following controls where identified which were already implemented in part - Authorisation management should be implemented, Physical access should be restricted through for example access gates, Data should always be classified, Physical pieces of information should be kept behind locked doors or in a vault, Server rooms should also be locked and hard disks with confidential information should be locked up and finally, Audits should be performed on the adherence to policy and procedures.

A general conclusion was that people see the world around them in which information is stolen, however they do not see the need to be careful with information they handle. Awareness training is required to remove this misconception.

DISCUSSION

To solve the research problem three main research questions where stated, the deliverables related to these questions will now be discussed to see if the research questions have been answered:

Which risks do organisations run as to social engineering?

To be able to identify social engineering risks the definition of social engineering is given in the introduction. Based on the knowledge gained on the findings and discussions, a risk assessment can be made. This *risk assessment* should be performed structurally this is also a component of the social engineering risk management model as in the discussion. When an organisation follows the steps in this model and more specifically the risk assessment this will help them to get a view on their specific social engineering risk. It however cannot give a general risk level, because of the great diversity in organisations.

The actual social engineering risk management model structures the risk management process and generates assurance for the management on their level of control over social engineering consisting of 10 steps - System and environment characterization, Objective setting, Threat & Vulnerability identification, Likelihood determination, Impact analysis, Risk Evaluation, determination & Response, Control analysis & Implementation, Supporting policy and procedures implementation, Information and communication management, Ongoing monitoring and evaluation. These steps can be related to the management process components of the Enterprise Risk Management Integrated Framework (ERM) of the Committee of Sponsoring Organisations of the Treadway commission (COSO) and therefore be implemented as part of this overall management process. The components are: internal environment, objective setting, event identification, risk assessment, risk response, control activities, information and communication and monitoring.

Therefore, this model is relatively elaborate and should be tailored to the organisation and/or incorporated in the organisations ERM process. Based on this social engineering risk management model and the observations from the research conclusions have been drawn and stated.

CONCLUSION

The paper discusses the social engineering risk management using a model in line with Enterprise Risk Management (ERM). The discussion started with the definition of social engineering risk management and its relevance and benefits to organisations; the limitation of social engineering risk in accordance with the organisations objectives. Also, the goal of implementing a social engineering risk management model based on existing risk management models is stated; to assist the organisation in managing the social engineering risk.

In conclusion, the social engineering risk management model could solve the research problem: The model is however still defined on a high-level and application in practice should show the actual usefulness. On this some recommendations for further research are stated.

REFERENCE

Alexander, M. (2016). Methods for Understanding and Reducing Social Engineering Attacks. *SANS Institute InfoSec, 1*(1), 1-34.

Barghuthi, N. B. A., & Said, H. (2014). Ethics behind Cyber Warfare: A study of Arab citizens awareness. *Proceedings of the 2014 IEEE International Conference on Ethics in Science, Technology and Engineering* (pp. 1-7). Chicago, IL: IEEE.

Bodhani, A. (2013). Bad: in a good way. *Institution of Engineering and Technology, 7*(12), 64-68.

Dempsey, K. L., Johnson, L. A., Scholl, M. A., Stine, K. M., Jones, A. C., Orebaugh, A., Chawla, N. S., Johnston, R. (2011). Information security continuous monitoring (ISCM) for federal information systems and organizations. *Special Publication (NIST SP)-800-137*.

Drevin, L., Kruger, H., & Steyn, T. (2006). Value-Focused Assessment of Information Communication and Technology Security Awareness in an Academic Environment. In S. Fischer-Hübner, K. Rannenberg, L. Yngström, & S. Lindskog (Eds.), *Security and Privacy in Dynamic Environments: Proceedings of the IFIP TC-11 21st International Information Security Conference (SEC 2006)* (pp. 448-453). MA: Springer.

Dudek, L. C. & Ruffin, L. K. (2006), *Social engineering & internal/external threats*. Washington: United States Department of the Interior.

Harnesk, D., & Lindström, J. (2012). Materializing Organizational Information Security. In C. Keller, M. Wiberg, P. J. Ågerfalk, & J. S. Z. Eriksson Lundström (Eds.), *Nordic Contributions in IS Research: Proceedings of the Third Scandinavian Conference on Information Systems, SCIS 2012, Sweden* (pp. 76-94). Berlin: Springer.

Krone, T. (2005). Hacking motives: High tech crime brief no. 6. *Australian Institute of Criminology, 6*(1), 1-2.

Lafrance, Y. (2004). Psychology: A precious security tool. *SANS Institute InfoSec Reading Room, 1*(1), 1-32.

Legg, P. A., Buckley, O., Goldsmith, M., & Creese, S. (2015). Caught in the act of an insider attack: detection and assessment of insider threat. *Proceedings* of *the 2015 IEEE International Symposium on Technologies for Homeland Security (HST)* (pp. 1-6). MA: IEEE.

Long, J., & Wiles, J. (2008). *No Tech Hacking: A Guide to Social Engineering, Dumpster Diving, and Shoulder Surfing*. MA: Syngress.

Luiijf, E. (2012). Understanding Cyber Threats and Vulnerabilities. In J. Lopez, R. Setola, & S. D. Wolthusen (Eds.), *Critical Infrastructure Protection: Information Infrastructure Models, Analysis, and Defense* (pp. 52-67). Heidelberg: Springer.

Madarie, R. (2017). Hackers' Motivations: Testing Schwartz's Theory of Motivational Types of Values in a Sample of Hackers. *International Journal of Cyber Criminology, 11*(1), 78-97.

Mahfuth, A., Yussof, S., Baker, A. A., & Ali, N. (2017). A systematic literature review: Information security culture *Proceedings of the 2017 International Conference on Research and Innovation in Information Systems (ICRIIS)* (pp. 1-6). Langkawi: IEEE.

McPhee, D. (2008). *Information Security Management Handbook* (6 ed., Vol. 2). NY: Auerbach Publications.

Milberry, K. (2012). Hacking for Social Justice. In A. Feenberg & N. Friesen (Eds.), *(Re) Inventing The Internet: Critical Case Studies* (pp. 109-130). Rotterdam: SensePublishers.

Nurse, J. R. C., Legg, P. A., Buckley, O., Agrafiotis, I., Wright, G., Whitty, M., Creese, S. (2014). A Critical Reflection on the Threat from Human Insiders – Its Nature, Industry Perceptions, and Detection Approaches. In T. Tryfonas & I. Askoxylakis (Eds.), *Proceedings of the Second International Conference, HAS 2014, Held as Part of HCI International 2014 Human Aspects of Information Security, Privacy, and Trust: Heraklion, Crete, Greece,* (pp.

270-281). Cham: Springer.*Rahalkar, S. A. (2016). Information Security Basics. In Certified Ethical Hacker (CEH) Foundation Guide (pp. 85-95). CA: Apress.*

Richards, G. (2008). Hackers vs slackers - control security. *Institution of Engineering and Technology, 3*(19), 40-43.

Saunders, M., Lewis, P., & Thornhill, A. (2012). *Research Methods for Business Students* (6 ed.). UK: Pearson.

Shanmugapriya, R. (2013). A study of network security using penetration testing. *Proceedings of the 2013 International Conference on Information Communication and Embedded Systems (ICICES)* (pp. 371-374). Chennai: IEEE.

Shin, L. (2017). *Be Prepared: The Top 'Social Engineering' Scams Of 2017*. Retrieved October 6, 2017, from https://www.forbes.com/sites/laurashin/2017/01/04/be-prepared-the-top-social-engineering-scams-of-2017/#4adc4fb7fec1

Singh, K. (2007). *Quantitative social research methods*. New Delhi: Sage Publications.

Smith, A., Papadaki, M., & Furnell, S. M. (2013). Improving Awareness of Social Engineering Attacks. In R. C. Dodge & L. Futcher (Eds.), *Information Assurance and Security Education and Training: Proceedings of the 8th IFIP WG 11.8 World Conference on Information Security Education, WISE 8, Auckland, New Zealand, July 8-10, 2013, WISE 7, Lucerne Switzerland, June 9-10, 2011, and WISE 6, Bento Gonçalves, RS, Brazil, July 27-31, 2009,* (pp. 249-256). Heidelberg: Springer.

Solomon, M. G., & Chapple, M. (2005). *Information Security Illuminated*. USA: Jones and Bartlett Publishers, Inc.

Straub, D., Boudreau, M.-C., & Gefen, D. (2004). Validation guidelines for IS positivist research. *The Communications of the Association for Information Systems, 13*(1), 63.

Sreejesh, S., Mohapatra, S., & Anusree, M. R. (2014). Business Research Design: Exploratory, Descriptive and Causal Designs. In *Business Research Methods: An Applied Orientation* (pp. 25-103). Cham: Springer.

Svensson, R. (2016). Exploiting Vulnerabilities. In *From Hacking to Report Writing: An Introduction to Security and Penetration Testing* (pp. 89-152). CA: Apress.

Tayouri, D. (2015). The Human Factor in the Social Media Security – Combining Education and Technology to Reduce Social Engineering Risks and Damages. *Procedia Manufacturing, 3*(Supplement C), 1096-1100.

Tse, D. (2004). Security in Modern Business: security assessment model for information security Practices. *Proceedings of the Eighth Pacific Asia Conference on Information Systems* (pp.1506-1517). Shanghai: AIS.

Tsohou, A., Karyda, M., Kokolakis, S., & Kiountouzis, E. (2010). Analyzing Information Security Awareness through Networks of Association. In S. Katsikas, J. Lopez, & M. Soriano (Eds.), *Proceedings of the 7th International Conference on Trust, Privacy and Security in Digital Business.* (pp. 227-237). Heidelberg: Springer.

Voiskounsky, A. E., & Smyslova, O. V. (2003). Flow-Based Model of Computer Hackers' Motivation. *Cyber Psychology and Behaviour, 6*(2), 171-180.

Warren, M., & Leitch, S. (2010). Hacker Taggers: A new type of hackers [journal article]. *Information Systems Frontiers, 12*(4), 425-431.

Watson, I. (2012). Digital Underworld. In *The Universal Machine: From the Dawn of Computing to Digital Consciousness* (pp. 259-283). Berlin: Springer.

Whitman, M. E. (2004). In defense of the realm: understanding the threats to information security. *International Journal of Information Management, 24*(1), 43-57.

Yildiz, M. (2007). E-government research: Reviewing the literature, limitations, and ways forward. *Government Information Quarterly, 24*(3), 646-665.

Ziccardi, G. (2013). Hacking and Digital Dissidence Activities. In *Resistance, Liberation Technology and Human Rights in the Digital Age* (pp. 73-123). Dordrecht: Springer.