Social Engineering: Towards A Holistic Solution

K.. Jansson and R. von Solms

Nelson Mandela Metropolitan University, Institute for ICT Advancement, Port Elizabeth, South Africa
e-mail: Kenny.Jansson@nmmu.ac.za1
rossouw@nmmu.ac.za2

Abstract

As most employees are information-workers nowadays, they are very vulnerable to various malicious attacks. However, some threat sources have realized that it is far easier to obtain wanted information directly from authorized users than using software or other means to obtain such information. This is generally referred to as Social Engineering. Therefore, organizations are at risk, because most information-workers are very vulnerable to socially malicious attacks. The objective of this paper is, therefore, to present guidance in the form of a flowchart which should give employees some guidance on how to act when faced with a potential Social Engineering attack. The flowchart was deduced from information gathered in an extensive literature survey. If followed correctly, it should reduce the risk related to Social Engineering significantly.

Keywords

Information Security, Social Engineering, Risk Management, Risk Assessment, Policies

1. Introduction

The main goal of most organizations is to make as much money as possible while keeping their clients satisfied. However, it is impossible to reach this goal if the clients cannot be assured that all the services provided by the organization are constantly available and that the information the customers entrust in the ‘hands’ of the organization, is handled with care (Whitman & Mattord, 2009).

Many organizations spend large amounts of money to ensure that their information is protected. However, the focus is unfortunately too often on Technology. It is commonly believed that a product will ‘fix’ everything, but unfortunately this is far from the truth (NSTISSC, 1994). Some important aspects (i.e. the human aspect) are often neglected.

Employees tend to believe that Information Security is not their concern, believing that this is the IT-Department’s responsibility. However, this is indeed not the case (Mitnick & Simon, 2002). Ensuring the well-being of the organization is the CEO´s responsibility (King, 2002). If services are unavailable when needed or sensitive information is compromised, unavailable or unprotected, the organization can in fact come to a standstill. This will, in turn, compromise the well-being of the organization (Von Solms & Von Solms, 2009). Therefore it is critically important that the organization creates safe environments in which the business can function (Whitman & Mattord, 2009). Organizations have employed various methods to create these safe environments. However, the importance of educating their employees about how information should be handled is often neglected. For example, a threat to the organization can deceive an employee into compromising sensitive information, unaware that this is against the rules of the organization. This is called Social Engineering (Mitnick & Simon, 2002).

A Social Engineer would make use of his social skills to gain trust with employees in order to obtain confidential information, such as passwords. However, the success of such an attack depends on how educated the employees of the organization are. Therefore, this paper will focus on a holistic solution in the form of a flowchart, helping employees how to behave when getting suspicious requests. However, in order to understand the flowchart, it is first necessary to understand some of the concepts of Human Behavior and Social Engineering.

2. The Human Element

The desire to be liked by other people is common to all humans (Mann, 2008). By being helpful to other employees, such as holding the door open when another employee has boxes in his hand, meets this desire. This is especially true for new employees who want to make a good impression on the "employee" carrying the boxes. However, the "employee" with the boxes, could actually have been an individual with the intention to do harm, who just pretended to be busy with boxes, in order to get inside the building. In contrast, the individual could also pretend to be a new employee who other employees in the organization do not yet know (Mitnick & Simon, 2002). Likewise, a new employee would also not be a suspicious person, should he ask too many questions (Mann, 2008).

As a real case scenario, Steve Stasiukonis, founder of Secure Network Technologies Inc., tells his story in an article by DarkReading (2006) about a penetration test on one of his clients. The client asked specifically that the human element be tested, as they had problems with employees disclosing sensitive information. Therefore, Stasiukonis uploaded a Trojan horse on a couple of USB sticks and scattered these in different areas outside the client's building. Once the employees showed up, they became curious, picked up the USB drives, and plugged them into their computers to see what was on them. The Trojan horse collected, as expected, a lot of sensitive information and emailed this back to Stasiukonis. After a few days, Stasiukonis, concluded that of 20 USB drives that was planted, 15 were found by employees, and all of them had been plugged into the client's computers. With this information, Stasiukonis could compromise the client's system. This client was, in fact, a credit union company. If this was a real attack, the company's customer-accounts could have been disclosed, resulting in unauthorized money-transfers to a potential attacker's account. This attack can also be referred to as a Social Engineering attack.

Social Engineering is the art of manipulating a victim into making certain decisions (Mitnick & Simon, 2002). These decisions are processed in the mind of people, in a way they are not consciously aware of (Mann, 2008). A Social Engineer exploits these decisions by using some kind of technique that will either exploit emotions in the victim or will exploit the victim’s cognitive or cultural biases (Gupta & Sharman, 2009). These biases are human errors that occur when the victim is making a decision (Cialdini, 2001).

3. The Social Engineer

Ian Mann (2008) defines Social Engineering as a way of manipulating people, by deception, into giving out information or performing an action. However, in order to manipulate an individual into disclosing information or to perform a certain action, the individual must (in most scenarios) first of all trust the Social Engineer. As mentioned earlier, the decision whether an individual will trust another individual, is influenced in the subconscious mind of the deceived, in a way that the deceived is not consciously aware of (Mann, 2008).

In the early days before Information Technology and Telecommunication had taken a stable ground, employees of an organization would base their decision of trusting another individual on the way individuals introduced themselves. At a bank, for example, a customer would have to physically go to the bank and be identified when withdrawing money (Abagnale & Redding, 1980). To perform fraud, a Social Engineer had to control the body language which includes posture and eye movements, as well as the voice. The Social Engineer also needed the skill to think rapidly and clearly (Mann, 2008). However, when telecommunication evolved and organizations such as banks adopted call-in-services, the customer could do his errands via telephone, thereby eliminating the need to have a trustworthy body language. To identify the customer, all that was needed was a little information about the customer and a code. To perform fraud this way, a Social Engineer could simply call the customer, pretending to be from the bank, and ask him for some information and the code, for whatever reason. The Social Engineer could then call the bank, pretending to be the customer, using the code and could then transfer money to an anonymous account (Mitnick & Simon, 2002).

In this age of Information Technology, employees must make decisions whether someone is trustworthy, not only face-to-face or via the phone, but also electronically via the Internet (Denning, 1998). However, people would live a difficult life if they always had to mistrust others (Mitnick & Simon, 2002). Social Engineers know this, and use the human nature of trust to deceive an organization’s employees or customers (Mann, 2008). However, when establishing trust, the Social Engineer uses some sort of method. As mentioned earlier, these methods include psychological techniques that exploit emotions as well as cognitive and cultural biases inherent in the victim.

A Social Engineer who uses ‘psychological triggers’ to exploit emotions, influences the victim’s emotions whereas a Social Engineer who uses cognitive and cultural biases exploits mental shortcuts that the victim uses when making decisions (Gupta & Sharman, 2009). Nevertheless, Gupta & Sharman (2009) divide the emotions into being Negative, Positive or Neutral.

Negative emotions precede unpleasant feelings in the victim and can provoke a fight or flight response, thus making the victim do what is possible to get liberated from the incident, which could involve breaking Policies and Procedures and disclosing sensitive information (Gupta & Sharman, 2009). In contrast to negative emotions, positive emotions are feelings that build a trusting relationship between the Social Engineer and the victim, making the victim more willing to comply with the Social Engineer's requests (Gupta & Sharman, 2009). Neutral emotions can make the victim feel less accountable to incidents. The Social Engineer can make use of neutral emotions by making the victim believe that a specific incident is not the victim's fault or exploiting a victim who is being irresponsible in the organization (Gupta & Sharman, 2009).

As mentioned earlier, the other way a Social Engineer can exploit a victim, is by influencing the victim's Cognitive and Cultural Biases. These biases are, as mentioned earlier, mental shortcuts that people use when making decisions in uncertain situations (Gupta & Sharman, 2009). These mental shortcuts are also called heuristics or rules of thumb (Cialdini, 2001). In general, these heuristics are quite useful, but sometimes they lead to severe and systematic errors. However, people cannot function without their heuristics as their lives would be too difficult if everything that was perceived, said, and done first had to be thought through (Tversky & Kahneman, 1974). As mentioned earlier, people would live a difficult life if they always had to distrust others (Mitnick & Simon, 2002). Psychologist Robert Cialdini (2001) explains this with the following statement:

"We can't be expected to recognize and analyze all the aspects in each person, event, and situation we encounter in even one day. We haven't the time, energy, or capacity for it. Instead, we must very often use our stereotypes, our rules of thumb, to classify things according to a few key features and then to respond mindlessly when one or another of these trigger features is present."

This statement leads to the concept of probability which resembles the subjective assessment of physical quantities such as distance or size. Tversky and Kahneman (1974) explain probability with how an individual perceives the distance of an object: "The distance of an object is determined in part by its clarity, the more sharply the object is seen the closer it appears to be." This is one example on how systematic errors are caused in the human mind. Distances are often overestimated when visibility is poor because the contour of the object is blurred. In contrast, distances are often underestimated when visibility is good, because the object is seen sharply. Thus, the reliance on clarity as an indication of distance leads to biases, or simply systematic errors. Therefore, a Social Engineer can exploit these types of biases and lead a victim into making a certain decision (Gupta & Sharman, 2009). However, Tversky and Kahneman (1974) also argue that prior-probability or, base-rate frequency also plays a big roll when an individual makes a decision. Should one have to choose between whether an individual is a farmer or librarian, the chances are bigger that the individual is a farmer, since there are more farmers than librarians in this world. Therefore, the base-rate frequency is based on odds.

The frequency (odds) and the probability that a threat might exploit some vulnerability can, therefore, be based on the victim's own belief. If, for example, an individual walks inside a building, and asks an employee if he can have his password, the probability that the individual is a threat (from the employee’s point of view) is then based on what the employee perceives. What the employee perceives is (as mentioned earlier) based upon how the employee has been influenced by the individual, who could be a Social Engineer.

To protect an organization’s information, countermeasures, or controls are (as mentioned earlier) needed in the organization. However, when it concerns guarding towards Social Engineering the focus should be at implementing Policies and Practices as well as educating all people in the organization. Therefore, to prevent a Social Engineer’s attack to succeed, a holistic solution is (as mentioned earlier) needed.

The aim of this paper is (as mentioned earlier) to develop a solution in the form of a flowchart which employees can use to help from falling victim to a potential Social Engineering attack. However, to know when to use this flowchart, the employees of an organization must first of all be able to recognize a potential attack. Therefore, it is critical that the employees are educated on the techniques a Social Engineer makes use of.

3.1. Social Engineering Techniques

A Social Engineer exploits (as mentioned earlier) Emotions or Cognitive and Cultural Biases inherent in the victim. However, there are many techniques associated with these exploits. Therefore, these techniques, partly identified by Gupta and Sharman (2009), will now be defined.

3.1.1. Exploiting Neutral Emotions

Carelessness: The Social Engineer takes advantage of the victim's lack of vigilance (Gupta & Sharman, 2009). For example, by looking for passwords written down and left out in the open, or that are thrown away (dumpster diving) (Lively Jr, 2004).

Diffusion of Responsibility: When the victim is made to believe that an incident is, or will not be, the victim's fault. In an organization, it is easy for end users to believe that security is not their responsibility, since there are individuals in the organization who are assigned specific information security posts (Gragg, 2003).

3.1.2. Exploiting Negative Emotions

Overloading: By overloading a victim with new information before previous information has been processed can reduce the victim’s ability to think an argument through (Gragg, 2003).

Urgency: During an emergency, employees often bypass Policies and Procedures, which gives the Social Engineer an excellent opportunity to get otherwise almost impossible requests approved (Mann, 2008).

Fear: For example, the Social Engineer pretends to be an important visitor or a close friend to the CEO of the victim's company and threatens the victim that the incident will be reported to the CEO if the Social Engineer's demands are not met (Mitnick & Simon, 2002).

Scarcity: When something is believed to only be available for a short time. For example, a Social Engineer sends emails claiming that the first 500 people to register at a Web site will win a prize. The Web site would simply have a field where users provide their company email address and a password for the site. Since many employees use the same password on different systems, the Social Engineer can, if lucky, get access to these employee's email-accounts (Mitnick & Simon, 2002).

3.1.3. Exploiting Positive Emotions

Reciprocation: This is based on the social rule that if someone does (or promises to do) someone a favor, then something is expected in return. Cialdini (2001) explains this through the following behavioral experiments. If two people are in disagreement, and one person yields on some point, the other person will feel compelled to yield as well. A Social Engineer can use the Reciprocation technique to trigger a positive emotional state by making two requests to a victim. After arguing for a while the Social Engineer would simply yield to one of the requests and then, the victim will feel compelled to yield to the other request (Gragg, 2003).

Building Trust: Building a trusting relationship could take time and is done by being in contact with the same person regularly. Mitnick and Simon (2002) describe a case where a Social Engineer called a video-store, requesting the name and number for the manager, as well as the number to the video-store's headquarters, ostensibly to thank them both for the good service experienced in the store. After retrieving the name and numbers, the Social Engineer called the headquarters, pretending to be the manager asking for a small favor. This was repeated many times over a period of a month. With this method, the Social Engineer had by then built up a relationship with the headquarters and could start requesting bigger favors. In this case, the bigger favor was a customer's credit-card number, which the headquarters gladly gave the Social Engineer.

Similarity: People like other people they believe are similar to themselves (Mann, 2008). If the victim shares the same thoughts or has the same interests and goals in life as the Social Engineer, the victim can get a positive feeling and thereby easier approve a proposed request (Mitnick & Simon, 2002).

Helpfulness: People generally want to help other people (Mitnick & Simon, 2002). Therefore the Helpfulness technique can trigger a positive emotional state when the victim feels motivated to help the Social Engineer (Gupta & Sharman, 2009).

Integrity: Employees have a strong tendency to carry out the commitments that they believe were made by their fellow employees. If, for example, a Social Engineer gets hold of a vacation schedule, he could claim that an employee, currently on vacation, had promised the Social Engineer something. The victim can then feel committed to carry out the request (Gragg, 2003).

Legitimacy: The Social Engineer makes the victim believe that the source, or the Social Engineer, is credible or legitimate (Gupta & Sharman, 2009). Mitnick & Simon (2002) relate a story about a Social Engineer who registered a Web site with the name "paypal-secure.com" and sent out legitimate looking emails to people who were Paypal users (a service where users can pay other users over the Internet) claiming that the users' credit-card information must be updated. When a user attempted to update the credentials on the Web site (believing it was a legitimate Paypal-site), all the information was redirected to the Social Engineer. This type of scam is often called 'Phising'.

Authority: According to Cialdini (2001), people have a tendency to comply when a request is made by a person in authority. For example, a Social Engineer could pretend to be a CEO or a friend to the CEO.

Conformity: If the victim believes that a request has previously been approved by other fellow employees, this makes the victim feel less responsible as the responsibility is extended to the other fellow employees (Lively Jr, 2004).

Curiosity: Tempting the victim with a desire to know or see something (Gupta & Sharman, 2009). For example, sending a message to a victim, with a worm attached, that offers something enticing, such as confidential information or free pornography. When the victim opens the attachment, the worm will spread over the network, retrieving and then sending all desirable information to the Social Engineer (Mitnick & Simon, 2002).

3.1.4. Exploiting Either Positive or Negative Emotions

Strong Affect: Triggers a heightened emotional state making the victim feel a strong sense of surprise, anticipation or anger (Gupta & Sharman, 2009). For instance, proposing a lottery-win could trigger positive emotions while frightening an employee that his job is on the line could trigger negative emotions. Therefore, strong affect can exploit either positive or negative emotions (Gragg, 2003).

Namedropping: Influences the victim to believe that the Social Engineer knows somebody the victim knows, by mentioning that person's name (Mitnick & Simon, 2002). Therefore, as individuals can feel both negative and positive feelings towards another individual, namedropping can exploit both positive and negative emotions.

Flattery: The Social Engineer makes the victim feel special (Abagnale & Redding, 1980). Dorf (1999) argues that if a person is being flattered, that person will have two possible reactions. The person will either think that the flatterer is lying and therefore experience bad, negative feelings towards the flatterer. Alternatively the individual will accept the flattering remark and believe everything the flatterer says, and consequently feel good, positive feelings towards the flatterer. Therefore, flattery can exploit both negative as well as positive emotions.

3.1.5. Exploiting Cognitive and Cultural Biases

Anchoring: For example, The Social Engineer asks directly for a password, and if denied, he asks what kind of system is being run. Once the more extreme request is established as a baseline, the less extreme case will seem more reasonable (Gupta & Sharman, 2009).

Representativeness: When stories contain details, they seem more believable. This phenomenon is called Representativeness (Tversky & Kahneman, 1974). For example, a Social Engineer may phone a victim, while pretending to be an administrator, and tell the victim that he is calling from the server room and sees strange activity on the network, and therefore needs the victim's password. Because the Social Engineer uses details like location, reason etc., the victim would be more likely to believe the Social Engineer, than if he only claimed that the password was needed (Gupta & Sharman, 2009).

Nevertheless, if any of the techniques are recognized, the employee should be extra suspicious. Thus, when an employee gets a request from an individual, and the request does not seem correct, the flowchart in Figure 1 should be followed.

4. The Social Engineering Flowchart

The Social Engineering Flowchart (Figure 1), deduced from all prior information gathered in this research, was (as mentioned earlier) created to help employees ‘do the right thing’ by giving some guidance on how the user should act when faced with a potential Social Engineering attack. Therefore, this section will focus on explaining the sequence of the Social Engineering Flowchart in detail. However, it is assumed that the necessary Technology and proper Policies and Procedures are already in place.

First of all, an individual will make some sort of request to a user in the organization. This can be some kind of favor or a query for some Information, etc. At this point, it must be concluded whether the individual is Internal or External to the organization. This is important so that it can be determined what kind of Information the individual can access. According to Whittman and Mattord (2009), Information should be classified as Confidential, Internal or External.

Information that is intended to remain within the organization and is only to be viewed by individuals with authorized access can be classified as Internal Information (Dulaney, 2009). Such individuals include: corporate employees, authorized contractors, and other third parties (Whitman & Mattord, 2009). These individuals are, therefore, Internal Individuals.

Information that has been approved by management for public release can be classified as External Information (Whitman & Mattord, 2009). Therefore, an External Individual is allowed to view any Information classified as External Information.

Access to Confidential Information must be strictly controlled on a need-to-know basis, even within the company. Therefore, Confidential Information is only to be viewed by approved Internal staff (Whitman & Mattord, 2009). However, if the individual is Internal, a procedure for identifying the individual must be conducted by the user (Mitnick & Simon, 2002). This identification procedure depends on what type of medium the individual is using.

When being Face-to-Face with the individual, the individual should be queried to show some type of identification. This identification should include a picture of the individual (Lively Jr, 2004).

If the individual is using a phone, it must be verified that the displayed phone-number matches the identity of the caller. Additionally, some type of code should be used. This code can be either a daily code (code that is different depending on what type of day it is) or a personal code that is specific for each employee (Mitnick & Simon, 2002).

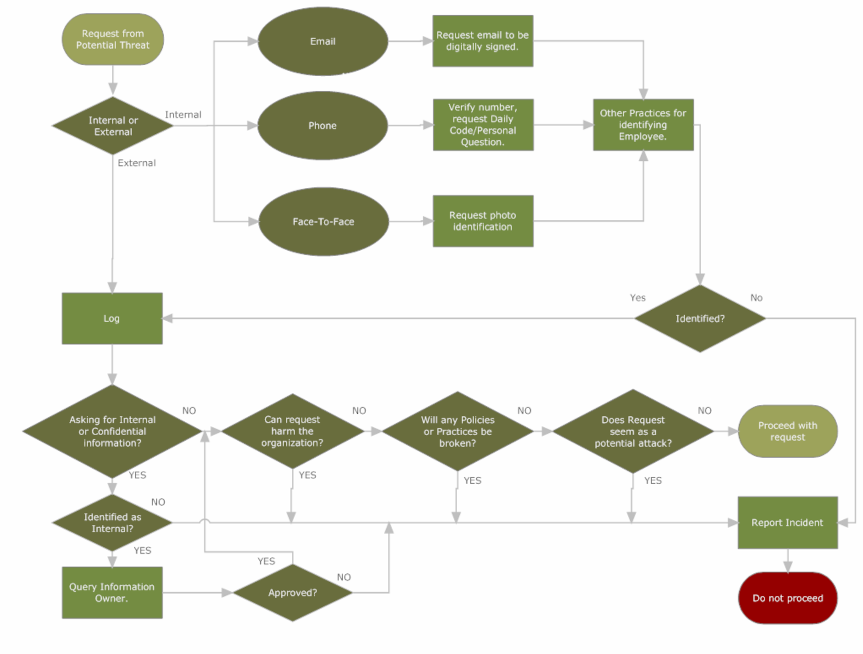
Request from Potential Threat
Internal or External
Internal
External
Email
Phone
Face-To-Face
Request email to be digitally signed.
Verify number, request Daily Code/Personal Question.
Request photo identification
Other Practices for identifying Employee.
Yes
No
Identified?
Log
Asking for Internal or Confidential information?
NO
YES
Can request harm the organization?
NO
YES
Will any Policies or Practices be broken?
NO
YES
Does Request seem as a potential attack?
NO
YES
Proceed with request
Identified as Internal?
NO
YES
Query Information Owner.
YES
Approved?
NO
Report Incident
Do not proceed

Figure 1: Social Engineering Flowchart

In the case of the individual using e-mail, it should be requested that the individual digitally signs the email with a certificate which provides proof that the email is originating from the correct person (Mitnick & Simon, 2002).

Then, if the individual claimed to be Internal and cannot be identified as being Internal, the incident should be reported and the request should not be proceeded with (Mitnick & Simon, 2002). Nevertheless, if the individual is identified as Internal, his details must be logged. This is also the case for External individuals.

External individuals should (as mentioned earlier) not have access to Confidential or Internal information. If this type of information is requested, the individual should be reported to security authorities and the user should not proceed with the request. However, if an individual identified as Internal requests Internal information, it can be handed over to the individual, but if Confidential Information is requested, the owner of the information should be queried as all such Information should have an owner assigned to it (Mitnick & Simon, 2002). The owner must approve whether the requested Information can be handed over to the individual or not. If the Information Owner has not given his approval, the incident should be reported to security and the request should not be proceeded with (Mitnick & Simon, 2002). However, if the Information Owner has given his approval or the individual is not asking for any Information, the next question (can request harm the organization?) can be considered.

If a request can harm the organization, that request should not be proceeded with (Von Solms & Von Solms, 2009). However, in many cases it can be hard to determine if something can do harm or not. Therefore, in the case of uncertainty, the manager should be queried for advice as the wrong decision could make the organization come to a standstill (Mitnick & Simon, 2002).

The next consideration to determine is if any Policies or Procedures will be broken by proceeding with the request as Policies and Procedures should always be followed (Whitman & Mattord, 2009). Therefore, if any of these will be broken the request should not be proceeded with and the individual should also be reported to the security department. However, if an Internal individual has a valid reason to omit or change something written in a policy, the owner of the policy, or responsible person should be queried for advice.

There are endless amounts of Policies and Procedures that can defend against Social Engineering and it would be impossible to list them all. It is important though that the end-users are taught how to protect themselves. For more information on these, the book The Art of Deception by Mitnick and Simon (2002) can be referred to.

Lastly, if a request seems to be an attack on the organization, the individual should, as in the other cases, be reported to security (Mitnick & Simon, 2002) and the request should not be proceeded with.

5. Conclusion

This paper explained the problem associated with Social Engineering. Social Engineering is a major threat nowadays as the human element is often neglected as part of securing an organization. People working in an organization are, therefore, very vulnerable to socially malicious attacks. However, if the right security measures are implemented correctly, this vulnerability can be reduced significantly. One of these security measures should include educating employees. There are several campaigns and awareness programs that have been raised to educate people. However, when a real attack actually occurs, it is often difficult for users to remember how to behave (Mann, 2008). Therefore, this paper proposed a solution in the form of a step-by-step flowchart that employees can follow to identify, mitigate or even prevent a potential attack. However, the flowchart has not been tested extensively in practice. Therefore, the authors of this paper propose future research in testing and improving the flowchart.

6. References

Abagnale, F. W., & Redding, S. (1980). Catch me if you can: the amazing true story of the youngest and most daring con man in the history of fun and profit. Broadway Books.

Cialdini, R. B. (2001). Influence: science and practice. Allyn and Bacon.

DarkReading. (2006). Social Engineering, the USB way. Retrieved July 04, 2009, from Dark Reading: http://www.darkreading.com/security/perimeter/showArticle.jhtml?articleID=208803634

Denning, D. E. (1998). Information Warfare and Security. Addison-Wesley.

Dorf, R. C. (1999). The technology management handbook (Vol. 49). USA: CRC Press.

Dulaney, E. (2009). CompTIA Security+ Study Guide (Exam SY0-201). (4, Ed.) Hoboken: John Wiley & Sons.

Gragg, D. (2003). A multilevel defense against social engineering [White Paper]. Retrieved April 10, 2009, from SANS Institute: http://www.sans.org/reading_room/whitepapers/engineering/a_multilevel_defense_against_social_engineering_920

Gupta, M., & Sharman, R. (2009). Handbook of Research on Social and Organizational Liabilities in Information Security. Idea Group Inc.

King. (2002). King Committee on corporate governance. Retrieved May 24, 2009, from University of KwaZulu-Natal: http://www.ukzn.ac.za/ukznms/King-ReportExec-sum.pdf

Lively Jr, E. C. (2004). Psychological Based Social Engineering. Retrieved August 29, 2009, from SANS: http://www.giac.org/certified_professionals/practicals/gsec/3547.php

Mann, I. (2008). Hacking the human. Hampshire: Gower.

Mitnick, K. D., & Simon, W. L. (2002). The Art of Deception: Controlling the Human Element of Security. Indianapolis: Wiley.

NSTISSC. (1994). National Training Standard For Information Systems Security (INFOSEC) Professionals. Retrieved March 10, 2009, from The Committee on National Security Systems: http://www.cnss.gov/Assets/pdf/nstissi_4011.pdf

Tversky, A., & Kahneman, D. (1974). Judgment under Uncertainty: Heuristics and Biases. Science , 185, 1124-1131.

Von Solms, S. H., & Von Solms, R. (2009). Information Security Governance. New York: Springer.

Whitman, E. M., & Mattord, H. J. (2009). Principles of Information Security (3rd ed.). Canada: Course Technolgy.