Social engineering assignment

Sociology

Social Engineering This research paper is primarily based on information gathered from secondary sources explaining what the term “ social engineering” is, how it is perpetrated, and the impact it has on individuals and corporations. It will also discuss ethical issues and action that can be taken by both individuals and corporations respectively to mitigate and minimize the risk of social engineering attacks.

Social engineering, in the context of information technology, is defined as “ gaining unauthorized access or obtaining confidential information by taking advantage of the trusting human nature of some victims and the naivety of others” (Gary B. Shelly, 2010). The methods adopted are similar to those used by con artist where individuals are tricked into divulging confidential information.

Social engineers mislead their victims into providing confidential and critical information that can enable them to perpetrate fraud. Social security numbers, user names, passwords, credit card details, bank account numbers and organizational charts are prime examples of target information that is used by fraudsters to commit a crime or in some case sell the information to other criminals. Individuals using social engineering techniques, or social engineers as they are commonly called, are essentially hackers.

The only distinction is hackers use technical methods like installing spyware on targets computers or networks to secure information, whereas the social engineers uses a combination of technical, social and psychological skills to carry out their attacks. The article Social Engineering Foundamentals: Hackers Tactics (Granger, 2001) shows that attacks can be carried out in both physical and psychological forms and can involve physical intrusion into the work place, over the phone and collection of trash (a. k. a Dumpster diving).

Items found such as documents and outdated or broken hardware components may contain crucial information which can be use to carried out attacks. Moreover, these methods can be in the form of impersonation, persuasion and more advance tactics known as: “ reverse social engineering”. Reverse social engineering is when the attacker creates a problem for a target company then offers their services to resolve the problem. While in the process of resolving the problem the hacker would collect critical information needed to launch an actual operation.

This method is a three step process involving “ sabotage, advertising, and assisting” (Granger). Furthermore, according to information obtained from Cisco’s website, some of the current trends in social engineering includes “ phishing” where an email is receive that appears to originate from a legitimate source and attempts to secure information, and “ pharming” which takes advantage of web users by redirecting the user to a false website that appears legitimate (Cisco, 2011). These attacks have resulted in some serious ethical issues for organization and individuals.

In particular in companys’ or organizations that are victims of security breaches, were confidential client or customer information has been compromised, the question may arise, should any and all affected parties be informed as required by most state regulations. Some corporations may find themselves in a dilemma particularly because possible disclosure of such information may lead to loss of confidence and ultimate demise of the entity. Moreover, these issues may also lead to question of regulation, whether more is needed, especially for those companies that deal with sensitive customer information.

On the on other hand, should an employee who is tricked into divulging sensitive information come forth and risk termination? These are all ethical questions that are difficult to address but would depend largely in part on individual cases. The impact of social engineering on individuals usually results in identity theft which can be very costly and difficult to resolve. For example to repair damage credit history may take many years even when all liabilities are settled. The FTC estimates as many as 9 million Americans have their identities stolen each year.

Organizations, on the other hand, are prime targets for social engineering attacks. As technological changes moves at such a rapid rate, many companies, especially, small businesses struggle to keep pace, and policies and procedures are developed haphazardly, if at all. However, information security poses a great risk and must be addressed if organizations are to avoid a range of unpleasant side-effects?? and sometimes significant financial losses. A 2007 study conducted by the Ponemon Institute on security breach revealed that “ average total cost per reporting company was more than $6. million per breach and ranged from $225, 000 to almost 35 million”. Moreover, according to an article published in one of the leading Information Security Magazines “ 85% of organizations experienced a data breach in 2008” (Raymond. Al, 2009). Finally, in conclusion entities need to take steps to minimize or reduce the impact of successful attacks by providing continuous employee education on new trends and developments in the industry. Additionally raising awareness and a culture of security vigilance is the most effective way of detecting and preventing social engineering attacks and security breaches.

Moreover, for organization's to survive in this day and age they should develop and constantly update a robust contingency plan that should cater for all sorts of information security incidents, including social engineering attacks. Moreover for individuals the issue of awareness and self education about current trends in information technology, security and privacy issues cannot be overstated. References: Cisco. (2011). http://www. cisco. com/web/about/security/intelligence/mysdn-social-engineering. html. Retrieved April 18, 2011, from www. Cisco. com.

Gary B. Shelly, M. E. (2010). Discovering Computers 2010: Living in a Digital World Complete. Boston: Course Technology: Cengage Learning. Granger, S. (2001, december 18). Social Engineering Foundamentals. Retrieved April 18, 2011, from http://www. symantec. com: http://www. symantec. com/connect/articles/social-engineering-fundamentals-part-i-hacker-tactics Raymond, A. (2009, October). An effective incidence response process. SCmagazine. Retrieved April 20, 2011, from http://www. scmagazineus. com. ——————————————————– [1].

This article, obtained from the Symantec corporation website narrates a true story of typical attacked carried out by security consulting firm using social engineering methods. [2]. Federal Trade Commission: is a governmental body with primary responsibility to protect consumer rights. http://www. ftc.

gov/bcp/edu/microsites/idtheft/consumers/about-identity-theft. html [3].

The Ponemon Institute is an IT security solutions provider that is now part of the Symantec group a leading IT security company; the manufacturer of Norton Antivirus program.