Adrian N
an9905@rit.edu
CSEC.468.01
Risk Management for Information Security
Project Group – Social Engineering

In the context of information security, human-based social engineering fraud, otherwise known as “human hacking”, is defined as the art of influencing people to disclose information and getting them to act inappropriately. The ideology of such an attack is that some of these cyber criminals consider it much easier to abuse a person’s trust than to use technical means to hack into a secured computer system. By tricking the target into giving them information, they exploit certain qualities in human nature. This methodology, along with the tendency for humans to be the weakest link in the security chain, creates a vulnerability that can have a serious operational impact. According to the paper titled, “Guide to Preventing Social Engineering Fraud” it states, “Social engineers also exploit a person’s natural tendency to avoid doing something wrong or getting in trouble. If an attacker can make an employee feel that he or she caused a problem or performed a task incorrectly, then the employee may become open to suggestion and thereby agree to compromise a policy or standard in order to correct the perceived error, which then leads to a breakdown in information security protocols.” This excerpt from the paper shows the psychological point of view of the science behind a social engineering attack. It speaks on the volumes that these attackers go through in order to achieve their goal through a non-technical gateway. This applies to risk management as due to social engineering attack success rate, it must be a big risk one should mitigate. Some countermeasures for combating these attacks are to conduct a data classification assessment to make sure each employee has access to things they need access too, and to make sure you can identify which employees are prime candidates for these attacks due to the access they hold to sensitive information. In terms of my project this paper can be used to help support my psychological study of social engineering attacks as I can speak on the manipulation part of the whole attack.

References

Guide to Preventing Social Engineering Fraud. (n.d.). https://www.gbainsurance.com/sites/default/files/2016-06/Social%20Engineering%20Guide%20From%20Chubb.pdf