A social engineering assessment is very important measure to understand an organisation’s security exposure. As human beings tend to make errors and are considered the weakest link in a security strategy, social engineering assessment can easily identify the key areas that we need to address in a timely manner. Hence, it’s imperative that an information security professional designs, organizes and carries out a successful assessment.

So, what are some important factors that security professionals must consider when planning this kind of review?

**Plan and Organize**

The first step is plan and organize your assessment. Think of the areas that you need to review and how to measure the security posture of each area in the best possible way. For instance, some potential areas to consider could be:

* Phishing attempts – how employees react when they receive suspicious emails and requests?
* Connecting to the company’s network in authorized areas in plain sight
* Attempts to enter unauthorized areas unaccompanied (to see the reaction of security personnel and employees)
* Asking for confidential information about the company or employees through emails and phone calls.

After you identify the key areas for your review, create scenarios that may arise. These are especially relevant for physical security mechanisms. Anticipate what may happen in each situation.

**Identify Attack Vectors**

Next is to identify all the methods you will use during the assessment, with each method linked to certain users. For example:

* Testing security guards by impersonating as someone relevant to the organization.
* Testing security guards by using tailgating test. This test should involve close monitoring of employees as they enter the building, especially during peak hours when high volume of employees enter.
* Testing accounting personnel through phishing tests by sending then an email that spoofs an executive’s office and requests to send last six month’s expense reports for review
* Testing an employee in IT by using an impersonation test. This could include a request by an employee for password reset.

Listing these attack vectors not only help steer the direction of the social engineering assessment but also help the management understand the step you took during the assessment.

**Execute and Report**

Here, you will execute the listed vectors in the previous step. Document the response for each of them to support the evidence. This evidence should include phone calls recording, email responses from phishing attacks, and undestroyed documents collected from dumpster diving activity.

Once you have all the results, make a detailed report. It should include the vulnerabilities discovered during the social engineering assessment and the recommendations on how to mitigate them.

Contact Aardwolf Security today for a comprehensive social engineering assessment for your organization.