Social engineering is not a test of technology. It is a test of user awareness!

Security Awareness Posture Assessment

There are several minor assessments that can be performed to help test the level of security awareness among your employees as it related to Information Security. The following is a list of the more popular services:

Password File Analysis and Report

We can either attempt to capture a SAM or password file from chosen systems or the client can provide the file. The password file will be audited for easily crackable passwords. We report the passwords that have been compromised and the timeframe an average attacker would have been able to discover these after obtaining the password file, thus giving a picture of the strength of passwords in place. The purpose of this process is to demonstrate the power, in terms of time gained, of strong passwords as well as measure the enforcement of the bank's existing password policy.

Pretext Calling

Pretext calling is used to assess the ability of staff members to not be tricked into giving out personal or confidential information. This is performed using "blind" and "semi-blind" pretext calling methods. During the blind phase, no information about the financial institution is provided to the testing team prior to performing the pretext calls. Also during the pretext calling, checks were made to verify that voicemail boxes were properly configured to require a password to be entered to access the voice mailbox system. During the semi-blind phase, a limited amount of customer information is provided to us by the financial institution. This information is used in an attempt to gain information from employees that would not normally be provided with that limited information.

Phishing Expedition

We usually send employees an e-mail, spoofing a client employee, that directs users to a duplication of the client's Website. From there, the employees will be required to reveal sensitive information, such as their network username and password. Our report summarizes percent penetration, shows print-screens of the e-mail and phishing site with annotations pointing out what should have forewarned the user that this was not a legitimate e-mail and/or web site. We also provide the user names and passwords for all users who failed the test. This summary, along with the print screens, are very useful in your information security awareness program.

Physical Breach Tests

To test physical access controls and related incident detection and response, testers will attempt to passively breach physical controls, if they exist, and gain access to the network from the inside. We pose as a member of your network support team, a telephone repair person, etc. The report describes the attempt at each location and the response, a summary report showing the percent of penetration, and recommendations.