CASE STUDY: MEASURING THE EFFECTIVENESS OF SECURITY AWARENESS TRAINING

**Situation**

More and more, companies are starting to enact various forms of employee security awareness training. They are starting to recognize the value in attempting to secure their people as well as their networks. We greatly encourage this trend, as it is not hacking that results in the most damaging penetrations into an enterprise's security system. It often is the work of an employee within the enterprise that causes the most harm. In most organizations, security measures are focused on attacks from the outside. The insider threat usually is ignored, although it is an important area of concern.

One company that recently came to us had been pouring significant budget into its training program. However, the director of security who administered the program had started to be challenged by upper management to justify the amount of money being spent. Management understandably wanted to get a better sense of its return on investment for security awareness. The director of security knew the program was working, but was unsure how to quantify its effectiveness. He turned to us for help. Our research and innovation (R&I) team developed a solution that would test and measure the program.

**Solution**

One of the ways that we drive our cutting edge management consulting is through the use of R&I. Our team decided on the use of social engineering techniques to test and measure the program’s effectiveness. We used a form of social engineering known as phishing. The goal of an email phish is to get the user to click a malicious link. During these assessments, when the user connects to the website, it resolves to a page that presents a message on phishing awareness. We are also able to track if a user clicked the link in the email.

In a standard phishing assessment, we typically impersonate an internal employee to trick personnel into visiting our sites. However, for this engagement, we created a series of emails with clues that the email was not legitimate. All of the clues were points that were previously covered in the initial awareness training. To those employees who were paying attention, they would be able to easily identify the emails as fake.
Results

We performed these phishing assessments for the client every four months. The assessments consisted of sending a statistically significant number of emails to employees across a broad range of departments and job classifications. In the downtime between assessments, the director of security implemented changes to his employee awareness training. Then when the next assessment was performed, the company had a baseline against which upper management could measure the effectiveness of the changes.

By tracking clicks throughout the year, we were able to generate and analyze a significant amount of data, and then present that data in a manner that was useful for the company. When you have quantifiable data, it is easier to make better decisions. The upper management was happy to have found a creative way to measure the program, rather than in the past where they just poured money in and hoped that it was working the way they expected.

The result of the assessments showed that through the training, employee awareness was improving measurably. As the assessments progressed and changes to the program were implemented, fewer employees were fooled into clicking our links. Management was now comfortable that they were not wasting their money. The director of security was able to maintain funding for a program that was helping to make the company less susceptible to attack.

This engagement is another example of a client bringing a problem to us that they were unsure how to solve. Our work with the client used research and innovation to not only identify a solution, but to enact that solution and provide a report to the client that improved its overall security posture.