Roundtable Summary – Security Awareness

Table Leader: Tracy Wilkerson
Participants: Steve Martin, James McQuiggan, ???

Key points from Discussion:

Annual Training for Compliance does not equal security awareness! It is the minimum. Security awareness is a “program”, not an “event”.

It’s important to have some measurement criteria if possible so you can see the trends. Is user behavior improving? How do we know? Phishing campaigns are one training method where you can objectively measure progress.

The most important thing you can do is to know what works for your company and tailor it to the various departments and participants. What works for a small company may not be effective for a large, multi-location company. It takes a while if you are new to a company to really understand what will motivate people and get their attention.

Integrate awareness into standard company communication vehicles that are already in place such as:

- Pamphlets for new-hire orientation
- Company Newsletters / departmental bulletins
- Bulletin Boards / plasma screens
- Internal “intranet” web pages

Alternate the topics but use a consistent theme for a period of time. That seems to reinforce the message. Tell them what good behavior looks like.

If you can connect the training to a personal benefit then people will take more of an interest. If you can use topics that they can relate to such as how to secure your Facebook page, how to secure your home router, how to secure your smart phone, how
to protect against identity theft, how to keep your children secure on the internet, how to keep track of your passwords, how to create good passwords (e.g., passphrases), etc.

If we feed them, they will come! Try a lunch & learn with a guest speaker.

If we give away free stuff, they'll be there. Prizes are even better!

One idea that has worked well in a large company is having a security rep in every department (Information Security advisors, ambassadors, etc.). You can provide them with detailed training and make their roles & Responsibilities clear. They represent security but can always call for advice or refer people to you for technical information, policy questions, etc. Give these reps some type of recognition at least annually. Make having a security rep a part of each manager’s performance goals so they have an incentive to have a security representative in their department. Hold periodic (e.g., monthly or quarterly) face-to-face meetings or Webex meetings with the advisors and listen to what they are saying. Are there common problems or questions? How can you provide service / value to help address these?

Gamification – how can we make it fun and motivate people to do more than the minimum? Really dig into the company culture and what motivates folks to act?

Consider the impact we can make by educating the younger generation about security. You can give talks to students in schools, talk with parents. Help the schools teach secure coding or help them integrate security into their technology curriculum.

Most important – never give up! It is an ongoing process.