Chapter 17 Information Security Awareness

Chapter Objectives

This chapter will discuss:

- Ensuring employees understand their role in security;
- The elements of information security awareness training;
- Training and its methods of delivery; and
- Change management.

17.1 Ensuring Employees Understand Their Role in Security

Throughout the book, especially in Chapters 12 and 13, the threats posed to an organization through parties attempting to trick employees into disclosing sensitive information were detailed. In Chapter 11, the task of communicating to an employee their responsibilities for protecting information and the range of possible consequences should they be found to have released information to an unauthorized party, especially through negligence.

17.1.1 Social Engineering

In Chapter 12, the "human element" was shown to be a key player in how information is released inappropriately. Leveraging intimate knowledge of human psychology, social engineers are far too often able to exploit our weaknesses to their advantage. As this book's author is an American, the psychological tendencies discussed are those of Americans and may or may not apply to another culture, or may need to be exploited differently in other cultures. Also, it is worth noting, the word *tendencies* is used purposefully, as not all Americans will behave in the same way.

17.2.2 Phishing

In Chapter 13, we covered the role phishing plays in the maturing world of email and instant message communication. This is also a type of social engineering, as the scam artists are attempting to capitalize on: a person's willingness to help others (someone in dire straits) , a person's fear (such as a credit card account being canceled unless specific information is provided to keep it alive) or greed (I'm in another country and need to transfer money out FAST! Give me your bank account information so I can send it to you and you can keep some of it.) These techniques don't work very often, but the fraudsters are becoming more sophisticated, as the case of the personalized credit union emails established. Even something as seemingly innocuous as clicking on a link sent in an email or instant message could risk exposing the user to a virus, spyware or keylogger.

17.2.3 Initial Employee Communication

Informing a new employee of the organization's expectations of them regarding their handling of controlled information is important, as it will set the tone for their work. A properly worded employee agreement stating the organization's policies on handling information provides the employer with "cover" should an employee violate its policies.

17.3 Information Security Awareness' Elements

While an organization has the right to protect itself against unauthorized disclosures, it also has an obligation to provide training to its employees to guide them as to what is approved and appropriate behavior and what is not as it pertains to handling information.

Peltier (2005), argues that learning for security awareness has three key aspects:

- "*Awareness*, which is used to stimulate, motivate, and remind the audience what is expected of them.
- "*Training*, the process that teaches a skill or the use of a required tool.
- "*Education*, the specialized, in-depth schooling required to support the tools or as a career development process."

In developing an information security awareness training regime, the organization's human resources department should work in conjunction