Chapter 11 Initial Employee Communication

Chapter Objectives

This chapter will discuss:

- The overall purpose of communication in establishing an employee's work environment
- Five types of information an employee could handle in the course of their work
- The role of employee agreements in establishing an employee's responsibilities to the organization regarding proprietary information
- Employee rights and responsibilities regarding organization-issued equipment and equipment brought onto organization premises
- The organization's policies toward monitoring employee behavior regarding personal communication while working, and
- The consequences an employee could face in the case of unauthorized information release or other unapproved communication behavior

11.1 The Overall Purpose of Initial Employee Communication

When a new employee joins an organization, it is important to establish a realistic picture in their mind of their rights and responsibilities with regard to their new place of work. For information security the real issue comes in, for most organizations, the balance between providing good internal and external responsiveness and protecting the organization from internal and external threats. The potential consequences of a security breach are so high that every reasonable precaution should be taken to guard against losing confidential or individual data. Initial and ongoing employee communication and training should be seen as a means to help employees understand their role in security as well as potentially inoculate the organization in the case of a breach.

Another aspect of security when an employee joins an organization is the decision that must be made by the company as to where to strike the balance between ensuring its security and imposing too many restrictions on its employees. Workers are willing to tolerate only so many constraints in relation to their level of compensation. A very fine line exists between keeping otherwise lazy workers vigilant and forcing good employees out of the organization because the level of monitoring they face every day is more than they are willing to endure.

Important: The author is not a lawyer and is therefore not able to render legal opinions or give legal advice. Terms used may not be the most appropriate ones when applied in a legal context and should be interpreted as coming from a layperson and intended for a layperson. All statements in this chapter and the book as a whole should be viewed as discussion points and concepts rather than legal advice, including those passages in which a licensed attorney is cited, as their publicly available works may contain a similar disclaimer. It is strongly recommended that you consult a licensed attorney in your jurisdiction should any question about relevant laws and precedents applying to your particular situation arise.

11.2 Some Examples of "Confidential Information"

An important question to ask and answer thoroughly is "What information, in isolation or in combination with other information, would compromise this organization?" In much simpler times, hard copies of documents and drawings kept in secure locations were the only records of an organization's confidential data, very few people had access to the areas in which the physical records were held and the only way to get the records out was to hand-copy them or smuggle in a camera to take a picture of the material. Now, of course, while access is limited and shredders have been deployed throughout many organizations, there are many more ways to access and make off with an organization's data. In answering this question, several types and sources of information must be brought into the equation.

Technical Information- As addressed in the discussion on social engineering elsewhere in the book, being able to gain access to a competitor's research and development, product, or other information will allow the