Chapter 12 The Human Element

Chapter Objectives

This chapter will discuss:

- The role of the human being in an organization's security,
- The concept of the "mosaic" technique of intelligence gathering,
- The idea of a "social engineer" and how they operate,
- Some ways a social engineer may be defended against, and
- How an organization can integrate the human element into its balanced scorecard.

12.1 Humans- The Weakest Link in the Chain

Con men, rip-off artists, scammers, snake oil salesmen, whatever you call them, there are people in our world whose chosen profession is to trick us into revealing information to them that they have no legitimate right to know for use to their advantage. As noted in the chapter on Physical Security, the first line of defense may be a locked door or, appropriate to the technical discussion earlier in the book, a log-in screen, but none of that matters if someone is able to bypass the defenses. In some cases, being able to gain the needed access is shockingly easy, as will be discussed later in the chapter. The type of theft may be thought of in two different ways. First, *direct theft* is when an intruder gains unauthorized access and is able to get away with a program, formula or marketing plan, for example that gives the information's recipient an advantage they otherwise would not have enjoyed. With such information, a competitor would be able to beat the developer to market or would be able to reverse-engineer the design or code in order to build their own "copycat" product with most of the research and development done for the cost of stealing the information.

The second type of theft may be referred to as *indirect theft*. This type of theft occurs when an individual or group of individuals accumulate sufficient information to be able to discern a competitor's confidential data or strategies without (sometimes, arguably) needing to commit an actual

crime. In fact, indirect methods may be used to enable a perpetrator to commit a direct act against an organization, as will be discussed in a moment when social engineering is addressed. The technique, known as constructing a "mosaic", is a powerful tool in intelligence gathering and analysis.

12.1.1 The Intelligence "Mosaic"

The American Heritage Dictionary (2004) defines "mosaic" as:

"1. (a) A picture or decorative design made by setting small colored pieces, as of stone or tile, into a surface. (b) The process or art of making such pictures or designs.

"2. A composite picture made of overlapping, usually aerial, photographs.

"3. Something that resembles a mosaic: *a mosaic of testimony from various witnesses.*"

As the definition moves from its most common usage (1) to least common (3), it becomes more relevant to the discussion at hand. The method describes a composite of information gathered and combined to reach a conclusion, based on independent inputs for analysis. A key technique in crime scene investigation is to ensure eyewitnesses talk with each other as little as possible, as their memories may be influenced through talking with other witnesses. While it may be more convenient to collect consistent input from all sources, there is a chance the collective memory will be incorrect. Rather, as social scientists have learned through training and other intellectually capable readers not having experienced the joy that is a formal social science education will remember from the popular and well-researched book *The Wisdom of Crowds* (Surowiecki, 2004), it is critical to gather as many credible and *independent* inputs as possible when evaluating a situation in dispute the adjudicator did not witness personally.

The field most commonly associated with the mosaic approach is espionage. The U.S. Congress' Joint Inquiry into the September, 2001 terrorist attacks noted that:

> "Intelligence analysts tend to reach conclusions based upon disparate fragments of data derived from widely-distributed sources and assembled into a probabilistic 'mosaic' of information. They seek to distinguish 'signals' from a bewildering universe of background 'noise' and make determina-