Chapter 9 Physical Security

Chapter Objectives

This chapter will discuss:

- How to decide on where to locate your organization's IT equipment,
- Some suggested ways employee identification may be accomplished to distinguish among various levels of access,
- How to handle an outgoing employee's physical access while they are transitioning out of the organization,
- How to handle visitors to the organization's facilities, and
- How the balanced scorecard for physical security could look at a high level.

9.1 Physical Security- Easily Overlooked

In today's world, the "cops and robbers" game of those trying to extract information from an organization versus those trying to prevent it is normally seen as a purely technological battle. While technology does indeed play a dominating role in the discipline, and IT managers likely see physical security as a mundane detail that is appropriately handled by operations, this chapter is included because it is absolutely critical for all connected with protecting an organizations' assets to understand that penetration attempts occur from many different angles. This chapter, the social engineering section and the discussion on what influences an employee's behavior while on the job are especially important in dealing with the human element of security. When the French were convinced they were going to be invaded during World War II, they built what they thought was an impenetrable barrier of firepower known as the "Maginot Line". As it turned out, however, the invading force attacked from another direction. Because the Maginot Line wasn't mobile, the defense was pointed in the wrong direction and rendered useless. This serves as a good analogy for IT security, in that the best defense against attack from one direction, over the network, is useless if the penetration comes from "behind the firewall".

9.2 Where to Locate Computer Equipment

Almost every organization will at some point be forced to deal with a disaster brought on by fire, water, or electrical surge. Policies for backup and disaster recovery are covered elsewhere, so the discussion here will focus solely on the optimal location for the actual IT equipment. Key factors to consider when making this decision are:

- How much control do you have over the layout of your space?
- Where are candidate sites relative to external entrances?
- To what extent is the environment for the site controllable?

How Much Control Do You Have Over the Layout of Your Space?

For most companies, their real estate will be leased rather than owned, which will limit the options on how the space containing the IT equipment will be set up.

Are there "drop" ceilings? Drop ceilings are ceilings for a room that purposefully create space between the true ceiling and that of the working area by placing a structure, usually a metal grid on which foam panels are laid, with enough space for workers to run wire to offices from the server room without it being seen in the regular working area. Access is covered in another part of this chapter, but if there are drop ceilings adequate care should be taken to ensure that someone with a ladder and some agility will not be able to remove one or two ceiling panels and bypass the access door to the server room without at least an alarm being triggered.

Are the floors raised? Another way to enable wire to be run is by the opposite technique of a drop ceiling, a raised floor. This option is somewhat less flexible, in that to change a wiring configuration carpet, at the very least, will need to be moved aside, but for what is likely to be a permanent setup it works very well. A telltale sign of a raised floor is a drum-like sound whenever a person weighing over 180 pounds (about 82 kilograms) walks by while wearing dress shoes.

How much space is available in the server room? This factor is becoming less and less critical now that space-saving hardware such as blade servers are available, but knowing how much space one has to work with