

## Chapter One

# People and Property

Before developing a security program, it is necessary to assess the people and property to be protected. We will begin with our most important concern, people — employees and tenants, contractors, and visitors — even the unwelcome or uninvited ones.

### People

Providing safety and security for the official work force (including full- and part-time contract workers and temporary workers) is the highest priority and a primary responsibility. Solely from an asset perspective (despite attempts to reduce reliance on particular individuals), an organization's work force remains one of its most valuable commodities. The loss or incapacity of key personnel could result in temporary or permanent loss of vital information and resources.

#### ***Public Image***

To assess personal risk, it is helpful to examine the organization's public image — with an objective and even cynical point of view. This assessment may produce a few surprises and a list of possible targets within a facility or organization.

During the year 2000, there were over 23,000 violent acts committed on various employees in all areas of employment in the United States, and these are just the ones that were reported.

Targets for assault include:

- **Within the general business community:**
  - Executives, officers, or other key personnel — vulnerable by virtue of their positions and actual or perceived responsibilities, which some employees, customers, or others could find sufficiently offensive to wish to injure or kill them. (The Unabomber killed and maimed out of a misguided sense of outrage at individuals he did not even know, but whom he believed represented industries injurious to society.)
  - Human Resources Personnel — susceptible because of their role in terminations of employment.
  - Employees at any level — as potential victims of violence connected with personal relationships.
  - Men — according to the Justice Department, are the victims of 80% of all workplace violence. Most are executives, managers, or other key personnel. Women share an increasing vulnerability in these same roles.
- **In specific industries or fields:**
  - Operators of facilities that generate (or are perceived to generate) pollution — electrical utilities, nuclear plants, petroleum refineries and chemical plants, and large-scale farming operations.
  - Other entities perceived as threats to the environment — lumbering companies involved in clear-cutting or lumbering old-growth forests, or electric utilities whose hydroelectric dams result in backwaters or drain wetlands.
  - Researchers whose work involves animals or breeders of fur-bearing animals — potential targets of animal rights activists.
  - Abortion clinic workers — vulnerable to violence from extreme “right-to-life” groups or individuals.
  - Healthcare workers who may be victims of a distraught relative or friend of a patient — and patients who may be accidental victims of an event.
  - According to the Bureau of Justice National Crime Victimization Survey, 69,500 nurses were assaulted at work from 1992-1996.
  - The National Institute for Occupational Safety and Health reports that 9,000 healthcare providers are attacked on the job every day.
  - Bureau of Labor Statistics figures for 1999 show that 43% of all non-fatal assaults and violent acts resulting in lost workdays across all industries occurred in health services.

- Government facilities and public buildings.
- Large facilities used for sports or entertainment venues.
- Transportation facilities, such as rail lines and railroad and bus depots and marshalling yards, airports, hangars, fuel bunkering facilities, ship docks, container facilities, warehouses, and storage facilities.
- Police, firefighters, and other security workers.
- Students and faculty — either as direct targets of disturbed individuals or as accidental victims of a collateral event.

It is nearly impossible to define all of the facilities and/or individuals who may find themselves at risk or in danger. Consequently, a security assessment committee or group must try to think in terms of protecting their facility and its users from completely undefined or unanticipated sources, as well as from the more commonly considered sources. The above list simply highlights some of the people and facilities that may be at increased risk.

### ***Invited Guests***

At any given time, there are likely to be other people, in addition to regular personnel, within a facility. Not only should the presence of these visitors be recorded from a security standpoint, but the host entity should recognize that it has assumed a responsibility for their safety and security. One method of helping both visitors and normal building users to avoid risks is by prominently labeling high-risk and/or restricted areas. Invited guests may include:

- Business guests: local or out-of-town associates and colleagues.
- Professional guests/consultants, such as attorneys, accountants, engineers, interior designers, and architects.
- Customers/clients.
- Outside contractors.
- Repair, maintenance, and construction personnel.
- Cleaning personnel.

### ***Uninvited Guests and Others***

The fact that people are not directly invited, but may be within a facility does not preclude or limit responsibility for their safety and security. Visiting family members, sightseers, sales persons, solicitors, and even potential “bad guys” are due a level of safety and security. Knowing who is in the facility and where they are should be a primary goal of a security program. The days of the “open” building or facility are over.

## Property

Although the safety and security of people is the highest priority of a security program, property is, by far, at the greatest risk and likely to sustain the most frequent loss or damage. There are essentially two forms of property for which a security program should provide protection: physical and intellectual property.

### *Physical*

Physical property is the most visible, vulnerable, and accessible to theft, sabotage, vandalism, or just plain loss. The loss of physical property may be a double- or triple-edged sword. There is not only the monetary value of the property, but the additional costs associated with replacement or repair, plus the time lost by personnel in securing a replacement or repair. In the case of a laptop computer, the loss extends to the value of stored data and software, as well as the possible misuse of stored information — both personal and business.

The security team should begin a program of review and assessment of all of the physical property within its scope of responsibility to determine:

- What is at risk.
- How critical it is to current and future operations.
- Whether to provide special protection for it.
- How to protect it.

Following is a short list of property types, which may stimulate further consideration.

- Buildings and structures — from storage sheds to aircraft hangars, compounds, campuses, docks, and vessels — together with their infrastructure components, such as roads; mechanical and electrical systems, including boilers, transformers, power transmission, distribution, and switchgear; water, sewer, or gas lines; fire and ejector pumps; and storage tanks.
- Within a structure or building there are various spaces, equipment, and components to which special attention should be paid. These include elevators and elevator hoist rooms and escalators, both of which require very heavy power loads; cooling towers, central chillers and circulating pumps of differing functions, incremental and/or fan coil units, Local Area Network and Wide Area Network Facilities (LAN and WAN), Main Distribution Frame (MDF) Rooms, Intermediate Distribution Frame (IDF) rooms, telephone demark rooms, Telephone Systems Entry Rooms (TSERs), Private Branch Exchange PBX equipment, telephone recording rooms, laboratories, clean rooms, refrigerated or critically cooled