building security through design

A PRIMER FOR ARCHITECTS, DESIGN PROFESSIONALS, AND THEIR CLIENTS

THE AMERICAN INSTITUTE OF ARCHITECTS

Building Security Through Design: A Primer for Architects, Design Professionals, and their Clients

The following excerpt describes how to systematically determine a client's need for security.

Defining Security Needs

Security assessments are used to define security requirements for the design of new buildings or for the retrofit of existing facilities. Although the scope and level of each assessment varies, its goal remains the same—to determine the acceptable minimum level of security protection for a given facility. Security assessments obtain answers to questions such as these: What is to be protected? What is the magnitude and nature of the potential threat? What are the vulnerabilities of what is to be protected? What measures can be taken to achieve the desired level of protection?

Security assessments use a combination of quantitative and qualitative techniques involving efforts such as surveys, data gathering, and expert evaluation. When the risk of hostile acts is greater, risk analysis methods draw upon information and data from intelligence and law enforcement bodies.

The basic components of a security assessment include asset analysis, threat analysis, vulnerability analysis, and risk analysis.

Asset analysis

In asset analysis, the assets to be protected are identified and prioritized. Assets include people, operations, information, and property. People, and their knowledge of operations, are considered the primary asset of an organization. Considered next is how the survival and functioning of an organization would be affected by damaged or lost information and property. The importance of various organizational functions to the survival of the organization can be used to prioritize the assets to be protected.

Here are a few considerations to be addressed in the analysis of assets:

- The nature of the asset needing protection (e.g., proprietary information, trade secrets, personnel records, etc.)
- The value of the asset, including current and replacement value
- Where the asset is located
- How, when, and by whom an asset is accessed and used

Threat analysis

A threat is any action with the potential to cause harm in the form of death, injury, destruction, disclosure, interruption of operations, or denial of services. Building threats include a number of hostile actions that can be perpetrated by criminals, disgruntled employees, terrorists, and others.

Building Security Through Design: A Primer for Architects, Design Professionals, and their Clients

Threat analysis defines the level or degree of the threats against a facility by evaluating the intent, motivation, and possible tactics of those who may carry them out. The process involves gathering historical data about hostile events and evaluating which information is relevant in assessing the threats against the facility. Some of the questions to be answered in a threat analysis include:

- What factors about the company or organization invite potential hostility?
- How conspicuous is the building?
- How vulnerable does the building appear?
- What political event(s) may generate new hostilities?
- Have facilities like this been targets in the past?

Possible methods of carrying out hostile actions include the following:

Bombs to damage or destroy building structures, which in turn can cause loss of life and injuries. The blast effects of a bomb are based on its size (referred to as load), its point of detonation (which may be outside or inside a building), the number of occupants in the building at the time of detonation, and the properties of structural and nonstructural building components.

Ballistic assaults directed toward building occupants, generally through the use of weapons such as handguns and assault rifles. Other ballistic assaults may use mortars, missiles, vehicles, and aircraft to inflict building damage with the intent of harming building occupants.

Biochemical tactics using biological and chemical agents to affect the health of building occupants. Such tactics include contaminating mailings and freight shipments and introducing biochemical substances directly into grates, air intakes, and other building openings and through service utilities such as water supply systems.

Vulnerability analysis

A vulnerability is anything that can be taken advantage of to carry out a threat. This includes vulnerabilities in the design and construction of a facility, in its technological systems, and in the way a facility is operated (e.g., security procedures and practices or administrative and management controls). A largely subjective process, vulnerability analysis identifies specific weaknesses with respect to how they may invite and permit a threat to be accomplished.

Examples of vulnerabilities related to site and building elements include:

- Surrounding terrain and adjacent structures

- Site layout and elements, including perimeter and parking
- Location and access to incoming utilities
- Building construction with respect to blast resistance
- Building circulation patterns and spatial arrangements
- Location of higher risk assets within a facility
- Lighting systems

Examples of vulnerability to technological elements and facility operations include:

- Employee and visitor access controls
- Locking controls
- Alarm systems
- Mail-handling protocols and procedures
- Access controls for service and maintenance personnel
- Information technology (IT) controls

Risk analysis

Risk analysis uses findings from asset, threat, and vulnerability analyses to determine which security measures can most effectively counteract the potential damage and losses produced by hostile actions. After possible security enhancement measures have been identified, the cost of each is determined. The cost of each measure is then compared to how it contributes to achieving the overall level of protection desired. From this evaluation, measures can be prioritized for consideration by decision-makers responsible for new design projects or retrofit initiatives.