

Vulnerability Analysis and Security Assessment

Contributed by Richard P. Grassie, CPP, President, TECHMARK Security Integration Inc.

Revised February 2007

The AIA collects and disseminates Best Practices as a service to AIA members without endorsement or recommendation. Appropriate use of the information provided is the responsibility of the reader.

SUMMARY

Understanding the fundamentals of vulnerability analyses and security assessments is critical to identifying and guarding against potential building security breaches. A list of common vulnerabilities and security assessment considerations are presented below.

KNOW YOUR VULNERABILITIES

Vulnerabilities are physical or operational weaknesses in building facilities that adversaries could exploit to carry out malevolent acts. The main purpose of vulnerability analysis is to identify the exposure of assets to potential threats. Asset vulnerability information is also used to determine the adequacy of existing protective measures and to assess the extent to which additional protective measures may be necessary.

Vulnerabilities are identified through surveys and plan reviews of existing buildings or proposed architectural designs for new buildings. The following statements of vulnerability, quoted from a security assessment prepared for a pharmaceutical manufacturing plant, illustrate vulnerabilities that many buildings have in common:

- Insufficient control and accountability of materials and finished products
- Insufficient control of company visitors and vendors
- Lack of protection for company's proprietary production edge
- Insufficient access control for critical areas
- Insufficient screening of employees for critical positions
- Lack of segregation of public and private space
- Insufficient procedures for guard force response to security or safety events
- Inadequate delineation and control of parking perimeter

- Insufficient access control and intrusion detection at main entry
- Lack of integration of systems technologies, personnel, and procedures
- Insufficient security operations and response procedures
- Insufficient employee background screening
- Insufficient screening of material or packages entering the building
- Insufficient segregation of interior operations
- Insufficient control and surveillance of parking lots
- Insufficient lighting of facility perimeter and parking lots
- Lack of control over vehicles approaching the building

THE SECURITY ASSESSMENT PROCESS

A building security assessment typically is performed as a distinct activity during a project's programming phase. For both new buildings and building renovation projects, security assessment findings are likely to affect the entire project delivery process. The project team should integrate selected security concepts, strategies, and measures into the design and documentation process for all disciplines (architectural, structural, mechanical, and electrical) and into all subsequent project phases of bidding and negotiation, construction, and building operation. The assessment process culminates in the determination of functional design requirements and recommendation of strategies for achieving the desired levels of protection, from which the client can select the strategies it deems most appropriate.

DEFINING THE SCOPE

A security assessment evaluates a client's ability to effectively and efficiently respond to a variety of security incidents, ranging from simple security violations to direct attacks on client assets, whether they occur locally or somewhere else. The following

tasks might be included in a typical scope of work for the assessment of an existing building (the same tasks can be adapted to designs of proposed buildings):

- Observe existing procedures and behavior with respect to the control of access and the screening of visitors at parking lots and main facility entrances.
- Assess external and internal access control procedures and measures for sensitive operations such as the data and communications centers.
- Observe and assess the vulnerabilities of traffic and parking plans and vehicle circulation patterns, paying particular attention to the safety and security of facility occupants and visitors.
- Identify high-risk areas and sensitive or critical operations; determine methods for protecting and monitoring such areas or operations; and assess the capability and effectiveness of the existing security staff to monitor and manage security operations in sensitive areas.
- Assess and evaluate the effectiveness of existing and proposed security measures and systems, including hardware, equipment, structures, staffing, and policies and procedures.
- Assess security lighting by conducting or simulating a night survey of lighting for video surveillance and personnel safety at main entrances, employee entrances, and parking lots.
- Conduct security surveys of the client site and facilities during normal operating hours, at night, and during hours of reduced operations, such as evenings and weekends.
- During nighttime and other after-hours surveys, observe routine recurring events—such as deliveries through the loading area, construction activity, and movement and habits of maintenance and cleaning personnel—to assess exposures, risks, and vulnerabilities posed by these after-hours operations.
- Review security reports of incidents at the client facilities, obtain local police crime and incident reports and area crime trend data, and extrapolate local government threat assessments to the client site. Factor all of these sources into an overall risk assessment.

- Inspect the physical perimeter, parking areas, and entrance gates of the client site to determine how effectively access is controlled and intrusion is deterred.
- Evaluate effectiveness of personnel security procedures, including personnel screening and facility operations.

TYPES OF SECURITY ASSESSMENTS

Security assessments can take many forms, but most examine the nature of the client organization and the assets potentially at *risk*: people, physical infrastructure (structures, building systems), proprietary information, and electronic infrastructure (computer and communication systems).

Assessments rarely focus on a single class of assets, but commercial building developers typically want assessments of base building assets (e.g., people, structures, building systems) and leave individual tenants to assess their own internal security needs with respect to access control and protection of proprietary information and computer systems. Corporations usually take a more holistic view of asset protection.

BASIC ELEMENTS

The following list, while not intended to be comprehensive, illustrates some of the elements to consider in conducting security assessments:

- Facility security control during and after hours of operation
- Personnel and contract security policies and procedures
- Personnel screening
- Site and building access control
- Video surveillance, assessment, and archiving
- Natural surveillance opportunities
- Protocols for responding to internal and external security incidents
- Degree of integration of security and other building systems
- Shipping and receiving security
- Property identification and tracking
- Proprietary information security
- Computer network security
- Workplace violence prevention

- Mail screening operations, procedures, and recommendations
- Parking lot and site security
- Data center security
- Communications security
- Executive protection
- Business continuity planning and evacuation procedures

RESOURCES

More Best Practices

The following AIA Best Practices provide additional information related to this topic:

- 09.03.01 Becoming a Certified Protection Professional
- 17.07.01 Understanding Human Behavior Leads to Safer Environments
- 17.07.06 Specifying Building Products for Building Security

For More Information on This Topic

See also "Security Evaluation and Planning," by Marco A. Monsalve and James R. Sutton, *The Architect's Handbook of Professional Practice Update 2003*. The *Handbook* can be ordered from the AIA Bookstore by calling 800-242-3837 (option 4) or by sending an e-mail to bookstore@aia.org.



Feedback

The AIA welcomes member feedback on Best Practice articles. To provide feedback on this article, please contact bestpractices@aia.org.

Key Terms

- Building performance
- Use design
- Security