

# Facility Management: Operational Security Factors

Contributed by Richard Grassie, CPP, and Behrooz (Ben) Emam, AIA, PE, CFM

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

Several factors influence the development of security operation plans. A few key factors include operating budgets, parking accommodations, internal security resources, and the management of multiple buildings.

## SECURITY OPERATIONS

Planning for building security operations should occur during the early stages of building design. Such planning can help identify and isolate a host of security considerations, including locations and types of doors, cameras, and access control points as well as their impact on daily personnel and material traffic flows. Other important considerations in the plan are points of egress and potential choke points during emergencies, location of isolation or restricted areas, visitor traffic flow, security policies and procedures, standards for security personnel, and types and scheduling of building safety checks.

## OPERATIONAL SECURITY FACTORS

Below are some of the major factors that influence the development of security operation plans and procedures.

**Facility type.** Security operations are most difficult to manage in public facilities, which usually require free access because the occupant's mission is at least in part to serve the public. In semipublic facilities such as hospitals, the task is somewhat easier because specific areas require heightened security and strict access control measures. In private facilities, the security operations depend much more on the business type and its organizational culture.

**Multiple buildings.** Typically, security operations for multiple buildings are handled by a small complement of security staff supported through security planning and technology applications. However, a single security officer can sometimes monitor multiple buildings from a single location, particularly after hours—for example, when occupants adhere to set procedures such as using scanning devices or card readers for access control.

In another situation, a building owner may place receptionists at the entry point of each building during business hours. After hours, a single security officer may be assigned to a control room along with one or more roving security officers.

**Parking accommodations.** Parking facilities can allow adversaries to commit personal and property crimes without detection. Enhanced security operations in parking areas are typically supported by intercoms or emergency phones at strategic locations and by cameras, scream alert detectors, and motion detectors in stairways. Closed circuit television (CCTV) cameras often enable surveillance of parking facilities. Complementing these technological applications are security patrols and security escorts upon request.

**Internal security resources.** Client or building user resources are important when designing a building with security in mind. Hospitals, high-rise buildings, museums, transportation centers, corporations, public agencies, and so on all have vastly different capabilities and resources to deal with security issues. Some establish detection and reporting systems with local law enforcement backup and investigative support. Others assume responsibility for the entire security operation, occasionally relying on local law enforcement for offender profiles, arrest, and incarceration.

**Operating budgets.** A one-year warranty is typically included with the installation of building security management systems. Thereafter, the owner must include sufficient funds in the operating budget for system maintenance and support. A reasonable cost estimate for maintaining a system for budget planning purposes is 10 percent to 12 percent of the capital cost of system installation.

## ABOUT THE CONTRIBUTORS

Richard P. Grassie, CPP, is president of TECHMARK Security Integration Inc., a Boston-based firm providing security design and technology integration services. Grassie has served as a consultant to Fortune 500, institutional, and

government clients in the United States and abroad. He is a board member of the International Association of Security Consultants and is past chair of the American Society of Industrial Security (ASIS) Security Architecture and Engineering Council. He has written numerous articles and conducts workshops and training seminars on security for public agencies and private industry.

Behrooz (Ben) Emam, AIA, PE, CFM, is senior manager for global facilities planning and engineering at Amazon.com. A registered architect, professional civil engineer, and certified facility manager, Emam has extensive experience in architecture and structural engineering; facility design, construction and project management; and emergency preparedness. He regularly teaches classes in construction and facility management and conducts seminars on seismic preparedness and disaster planning.

## RESOURCES

### More Best Practices

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

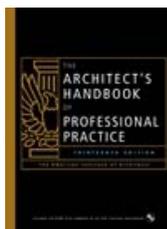
- 03.01.02      Becoming a Certified Protection Professional
- 11.10.01      Understanding Human Behavior Leads to Safer Environments
- 11.08.06      Facility Management: Building Security Access Control Measures

### For More Information on This Topic



This article is excerpted and adapted from *Security Planning and Design: A Guide for Architects and Building Design Professionals*, by the American Institute of Architects.

See also “Security Evaluation and Planning,” by Marco A. Monsalve and James R. Sutton, *The Architect’s Handbook of Professional Practice Update 2003*



See also the 14th edition of the *Handbook*, which can be ordered from the AIA Bookstore by calling 800-242-3837 (option 4) or by email at [bookstore@aia.org](mailto:bookstore@aia.org).



### Feedback

The AIA welcomes member feedback on Best Practice articles. To provide feedback on this article, please contact [bestpractices@aia.org](mailto:bestpractices@aia.org).

### Key Terms

- Building performance
- Use design
- Security