AIA Best Practices:
A client's-eye-view of building security

Contributed by Joseph Brancato, AIA

Summary

Clients are primarily and understandably focused on the day-to-day protection of employees and facilities. As their awareness of the need for security increases, they become more concerned about issues such as business continuity and the preservation of data, intellectual capital, the corporate brand, and the corporate image.

Clients often seek customized yet flexible solutions that can be implemented with minimal inconvenience and at a reasonable cost as well as "sensitive" or nonintrusive integration of security equipment and systems into the physical environment. The following information may increase understanding of clients' typical concerns.

Business continuity

Immediate loss of revenue is only the most obvious effect of business interruption due to a sudden event such as a natural disaster, facility damage, utility service interruption, loss of access to an otherwise unimpaired facility, or unsafe environmental conditions. The longer an enterprise cannot function, the greater the risk that it cannot resume functioning.

Beyond the immediate impact on the company's bottom line, concerns include the emotional and financial impact on employees, public perception of the company, and the possible loss of confidence and trust of clients. To guard against the possible disruption of business, it is important to recognize that different strategies are likely to be needed to respond to each type of event.

Protecting data and intellectual capital

Critical information needed to sustain business operations or restore operations after a crisis must be protected. Information and data must also be protected against possible security breaches. Many businesses address this issue through data redundancy (onsite and offsite) and by merging their security and information technology departments. Understanding which functions and datasets are critical, and how quickly systems must resume operations is the first step of preparing a disaster recovery plan.

Convenience by design

If security procedures or systems are inconvenient or anxiety provoking, people will resist them or eventually find creative ways to bypass them. Systems or procedures that are meaningless hassles—or perceived as such—are of little value. Human behavior and response to security must be considered. Holistic approaches to security may create safer environments while contributing to occupants' sense of safety and well-being.

Corporate brand and image

Placing a company's corporate identity on a building exterior is a popular marketing tool but can increase the risk to the building's occupants. In addition to the marketing considerations, each client must decide whether such visibility might pose an unacceptable risk.

Initial impressions

Most organizations wish to create an inviting atmosphere for their facilities. Many place security features at points of access to elevators and tenant spaces so that visitors may enter building lobbies before encountering security barriers. When a more visible security presence is desired, the barriers are located at the building entrance or even outside.

Urban properties tend to opt for a welcoming lobby atmosphere, while suburban facilities are more likely to restrict access to building interiors. Restricted building access allows more security personnel to be deployed on the property surrounding buildings.

Customized yet flexible solutions

Security elements may need to be customized to a specific site to create appropriately safe workplaces. Security needs will vary from city to city, from building to building, and even from business to business within a single building. No single solution can be applied to all. Examine every facility from a variety of user-specific perspectives so that design solutions are appropriate to the security challenges presented.

Cost implications

Security is not free. Financial considerations limit the level of security established for a building. Because the cost can be substantial, particularly to retrofit existing facilities, most security considerations will be subject to rigorous cost-benefit analysis. The surest way to get management support for a security strategy is to raise awareness of the likelihood of a security threat, its likely financial impact, and the benefits of a safer environment.

About the contributor

Joseph Brancato, AIA, is a co-managing principal for Gensler's Northeast and Latin American regions, and co-chairman of the firm's Board of Directors. He is active in talent development and mentoring, and shaped Gensler's gConnect program, which focuses on professional development for next-generation leaders in the firm.

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.

About AIA Best Practices

AIA Best Practices is a collection of relevant, experience-based knowledge and expert advice on firm management, project delivery, contracts and more, aligned with the *Architect's Handbook of Professional Practice, 15th edition*. See the full AIA Best Practices collection at aia.org/aia-best-practices.

This article corresponds to:

Architect's Handbook of Professional Practice, 15th edition Unit 1 - The Profession
Chapter 10 – Design Project Management
Section 05 – Design Phases