Access control and the continuity of the corporate business

Guest commentary

By Elvis Polanco - **05.2006**   📧 email

One of the major dilemmas facing corporate security managers, particularly in New York City after Sept. 11, 2001, is how to design an effective access control program for their properties while ensuring that the continuity and fluidity of the operation of the businesses therein would not be compromised. Security managers of properties with existing access control programs had to answer questions relative to improving the program to be more effective in deterring the malicious intents of criminals, ranging from the common con artist to the office intruder to the potential suicide bomber. Although the phenomenon of suicide bombers has yet to reach the shores of America, security managers have no choice but to design the access control programs with every possible criminal element in mind.

Elvis Polanco

OPTIONS ABOUND

Several access control options became available almost immediately. The most aggressively sought after appeared to be access turnstiles at elevator lobbies. Other properties settled for handheld ID scanners, while others simply did absolutely nothing and remained without an effective access control program. Properties that did not change from an unrestricted access control program were in effect "telling" the terrorists that despite the horrors of 9/11, their way of life would not be regulated in any way by the actions of terrorists.

Faced with the implementation of new access control measures, security managers pursued several avenues introduced by professional security consultants and law enforcement agencies. The changes ranged from simply having one main entrance/exit into the facility to funneling tenants and visitors to different corridors leading to elevator lobbies. Properties with internal ATM vestibules leading from commercial banks had their internal vestibule doors permanently secured or equipped with motion sensors and cameras to prevent unauthorized persons from circumventing the established access control measures. Others created visitor centers and messenger centers to ensure that only individuals with proper credentials had access to the property.

With limited budgets, even after 9/11, security managers sought the best deal possible and turnstiles were the best solution under the circumstances. Regardless of their design, turnstiles are aesthetically unattractive in multi-million dollar lobbies and are customarily designed for the average size person.

In one-tenant proprietary buildings, the employees have little say in what access control measures are implemented and are forced to accept the designed and approved program. However, in multi-tenant buildings that house companies that lease square footage for astronomical prices, their input is not only important, but also necessary for the successful implementation and maintenance of the access control program.

Companies, regardless of the state-of-the-art technical security equipment implemented, realized that personnel were as important, if not more important, than the technical security under consideration. This approach is critical to maintain the person-to-person interaction that would be lost with turnstile-dependent access.

ALL IN THE CARDS

Handheld ID card readers allow the familiar face of the security officer to remain in place, while registering the ID cards of tenants and visitors. The handheld card readers are more expensive in the long run because they must be operated by security officers. However, more important than the expense involved, is the sense of security and flexibility that officers add to the big picture. Technology, as it stands, has yet to program turnstiles that can negotiate with the president of a tenant company, who happens to have recently arrived from an overseas trip with several suitcases and inadvertently forgot his ID in a foreign country. The security officer has the discretion to allow him access, as opposed to a turnstile, that cannot understand the VIP's dilemma. The security officer brings a human element into the equation, an element that does not exist in interactions with computerized access control mechanisms.

Most tenants understand the need for improvements in access control; however, they feel that too much intrusion is both personally and professionally unethical and unacceptable. Many feel that their time of arrival and departure are being recorded for the sole purpose of

having their employers track their workday. However, when it is explained to the tenants that the purpose behind the use of access card readers is to ensure that the "right" persons are accessing the property, they understand and refrain from further challenging the program.

It appears that executives have accepted the fact that access control programs are now a permanent fixture in corporate office buildings. They will welcome an access control program that will not have a negative impact on their business continuity, and security managers must listen to their concerns in order to create the ideal security-conscious and company/employee-friendly working environment . . . a combination that is sure to stand the test of time.