Rising High with Security

By RICHARD H. CANTOR, CPP

Businesses operating in a high-rise, multitenant environment may expect that security has been built in by the developer. Often, the developer's real concern is for the appearance of security, rather than for genuine safety. Such was the challenge faced by Amerigard when it was hired to design a comprehensive building security system for a twenty-two-story commercial building in New York City. The building was to be occupied by a number of independent companies, most of which were expected to have high-value assets. ◆ The building owner's only concern was that security be provided to make the building attractive to the targeted market—high-asset tenants. He wanted to spend as little as possible on security. Worse, his project manager and partner expressed the opinion that a security system was a waste of time and money because even if it worked, "the boob behind the desk would make it useless." By the "boob," he was referring to the concierge (they didn't plan to hire security personnel) and by "make it useless," he meant turn the security system off, not use it, or bypass it. ◆ To say the least, this was not the ideal situation in which to have to design a security system but, in truth, it was not so different from the challenges many security professionals face in trying to provide good security with limited funding and little support. Such challenges required a plan that minimized expense and maximized creativity.

Faced with little funding, security found a strategy for sound security.

ILLUSTRATION *by* GUY BILLOUT

Amerigard knew immediately that it had a number of problems to overcome. A major one was that the system would have to work in a manner so that it could not be rendered ineffective, even with a "boob behind the desk." In security parlance, the system had to be fail secure. Yet the system also had to be tolerant of the commercial use of the building, which has heavy tenant traffic with high peaks at opening and closing times.

Even though the building owner wanted only for the system to look good to prospective tenants and did not care if it really worked, as security practitioners, we had an ethical obligation to make the system work and to protect the owner from liability and his own potential negligence.

> The project manager thought security was a waste of money because "the boob behind the desk would make it useless."

A major security consideration in such a situation was access control. And a large part of our efforts focused on the access control system considerations and design for this project. We had to consider the building staff and tenants as well as visitors, contractors, delivery people, after-hours security officers responding to tenant alarms from a variety of independent companies, and, of course, criminals.

Against this background, we set out to design a security system that would meet the physical demands of the building, create an audit trail for accountability, and follow our criteria for accommodating conflicting demands, potential change, and the vagaries of human behavior.

In designing an access control system, the first group we had to consider were tenants and building staff. A number of issues arose immediately. Tenant personnel change constantly and so does the building staff. During peak traffic times, when tenants flow into and out of the building, they become intolerant of delays. The concierge can easily become distracted during peak traffic times. Tenants vary in age, temperament, and dexterity, which can affect their ability to use access control systems. In addition, tenants frequently lose, forget, and misplace access cards; and people in all settings abuse access control systems by propping open doors, tailgating, and holding entry and exit doors open for others.

The second group we had to accommodate included visitors, delivery people, and contractors—those needing temporary access to specific locations within the building for varying amounts of time during normal business hours. The third group we had to consider was composed of after-hours visitors, alarm company officers, and tenants wanting reentry after closing the building.

This last group presented a particularly perplexing problem from a liability standpoint. The building was to have many tenants with millions of dollars in assets, such as cash, jewelry, and art, making it a target for criminals. The owner did not want to admit anyone after hours because he did not want any potential liability if the concierge inadvertently admitted a criminal onto the premises.

But locking out everyone after hours was impractical and actually increased the owner's liability in some circumstances. For instance, if security officers from a tenant's alarm company were denied access to investigate an after-hours burglar alarm signal, the owner could be liable for an ensuing loss. The goal was to maintain good access control and minimize the owner's liability for after-hours entries.

To further complicate the job, the budget was limited to an amount that would cover equipment only for the lobby, the architect presented severe aesthetic restraints, New York City was revising its fire code, and the Americans with Disabilities Act (ADA) required compliance. Other than that, the job was a piece of cake.

To begin the project, we broke the system down into components and worked toward the best solution for each part, then we integrated those parts. These parts included:

- Access control processor, readers, and programming
- Access control barriers
- Surveillance/video system
- Intercom system
- Alarm system
- Door control
- Emergency overrides/contingency planning
- Procedures

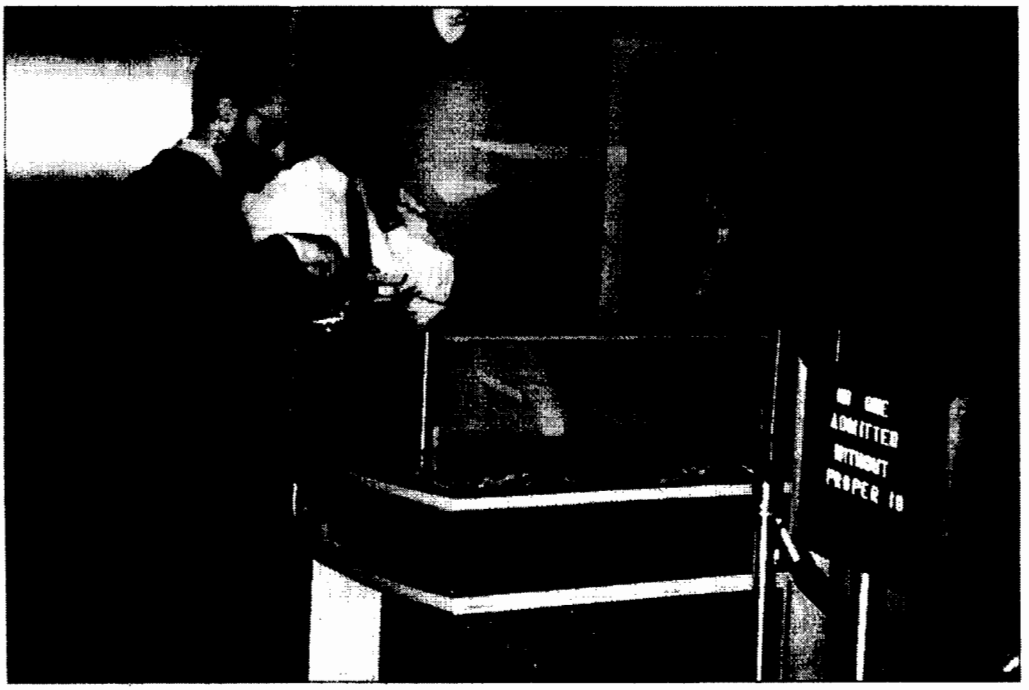
Selecting access control equipment may seem like an easy task since a variety of companies make excellent products, but it is also easy to make costly mistakes in selecting an access control manufacturer. The most important consideration is not the hardware, but the programming and software options available. Will the processor do what it is supposed to do, and is it flexible enough to accommodate future changes?

A second important consideration is the level of support the access control manufacturer can provide and the cost of that support. Have the product and software been in the field long enough for the bugs to have been eliminated? What is the warranty policy, and how financially sound is the manufacturer—will it be around in the future?

Among the features we considered important were proximity cards and readers for the combined benefits of ease of use, speed of traffic flow, and high security with modest costs. Other desired options included global antipassback and real-time. The real-time feature displays who is in the building and where they are at any time. Global antipassback permits the system to track all entries and exits, even if different doors are used. It gives tenants the convenience of being able to come and go by whatever point is easiest for them at any moment. The manifest can also be used by the concierge to determine which offices are opened and closed and to track the whereabouts of contractors, delivery personnel, and visitors throughout the building.

The access control barriers themselves became a major issue. Leaving aside the aesthetic considerations—which turned into a miniature war between the owner, the architect, and the manufacturer—we had to focus on the possibility that the revised fire code and the ADA would prohibit the use of turnstiles in the building's lobby.

We decided to use optical barriers in pedestrian lanes. While turnstiles have a more significant presence and prevent more user error, we could not risk delaying the certificate of occupancy in the event of code changes. Moreover, the major drawback with either optical barriers or turnstiles remains the same: Neither is effective if not attended. Either can be jumped over or crawled



After tenants authorize guests to enter the building, visitors are issued temporary access cards. The cards allow them to enter but not to exit without a buzzer sounding. The buzzer alerts the concierge to retrieve the access card.

under if no one is paying attention.

To make the barriers more effective we added a curtain motion detector that extended from the ceiling to the floor across the center of the lanes. This approach prevented anyone from circumventing the system by jumping over or crawling under the turnstiles.

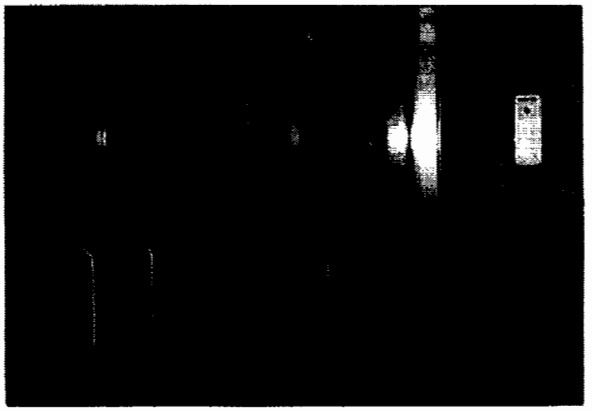
Once our access control system was finalized and the pedestrian lanes were selected, we had to determine how a violation would be handled under various scenarios from a simple mistake to armed criminals overpowering the concierge. The only open access to the upper floor was from the automatic (unstaffed) elevators. All doors leading from the lobby were to be secured by electronic locks and tied into the access control system.

Since no physical barriers to entering the elevators were present during business hours, we chose to tie the signal from any access violation into the elevator control. If a violation occurred, the elevators would be stopped automatically on the lobby level. Elevators already above the lobby would continue to run normally until they returned to the lobby and then they would be held also.

Once held, the elevators would not respond to any calls until released by a personal ID code entered by the concierge at the console. This procedure has many advantages. There are no barriers whatsoever that could invoke the concern of fire officials. Tenants are quickly motivated to use the system properly since their carelessness only delays them and fellow tenants, enjoining embarrassment, annoyance, and peer pressure.

The concierge is kept on his or her toes, because when the concierge is inattentive with visitors, the annoyance is directed at him or her. Too much dereliction of duty will bring the wrath of tenants to bear on the landlord to hire someone more competent. Thus, there is a built-in mechanism that promotes proper use of the system, attention to one's duties, and accountability—every time the system must be reset the event is logged by time, date, and individual.

Finally, even if the concierge is overcome by a criminal or injured, criminals still cannot gain access to the building. If compelled to enter a reset code, the concierge has a duress code with which to do so, which immediately signals our central station for response. Were criminals to overpower the concierge and use stolen cards to enter the building, an emergency duress signal would be transmitted within minutes.



All after-hour entries require dual control. Along with the access card, a video-image file is incorporated so that the concierge can verify the identity of the person entering the building.

During the day, when visitors arrive, the concierge confirms with the tenant via a video intercom. If the tenant authorizes the visitor, the concierge stores the visitor's picture on a video-image file, notes the person authorizing the visit, and issues a temporary access card that will allow the visitor in but not out. When the visitor exits, a buzzer sounds, alerting the concierge to retrieve the access card. (Access control violations on exiting cause an audible alarm but do not affect elevator operation.) For both access and liability, this is a dual-control function involving both the tenant and the concierge.

At night, access control strategy in the building changes considerably. At the scheduled building closing time, the access control system automatically activates the electromagnetic locks on both sets of entry doors (inner and outer). Anyone leaving the building can simply walk to the inner vestibule door on the right of the lobby, push the exit button, open the door, and proceed into the entry vestibule. When the inner door closes, the outer door may then be released in the same manner, and the person exits the building without assistance or having to use an access card.

To enter the building after hours, there are two procedures: one for tenants and

staff and one for visitors. The concierge has no control of the outer doors and the tenants and staff have no control of the inner doors. People with valid access cards wishing to enter the building must use their card, which opens the outer door only. The person then picks up the video intercom and calls the concierge to release the inner door.

In this manner, all after-hours entries require dual control. No lost or stolen access card can enable criminals or unauthorized personnel to enter the building after hours. Furthermore, a video-image file is incorporated into the system. Even if a new concierge is on duty, he or she can verify visually that the person seeking entry is the person to whom the card is assigned.

> The architect vetoed installing any physical barriers, so we installed a curtain motion detector to partition the entry vestibule.

This video-image file is also helpful during the day. It gives a new concierge a means of verifying that the person using an access card is the person to whom that card is assigned, and it also enables him or her to quickly and positively identify anyone who has lost an access card and needs a new one.

Additionally, it enables the creation of an accurate video audit trail created by a split recording of the person entering the building on one side of a videotape and the stored image of the person assigned to the card on the other. A quick and accurate record is made of everyone who enters the building and is available for review as necessary.

The system is further designed so that after-hours visitors are submitted to a similar dual-control entry. The visitor presses the intercom button on the outside of the building. This action connects the individual to the concierge, who can ask the visitor which tenant he or she wants to see.

Since the concierge has no way to release the outer door, he or she connects the visitor to the tenant via the intercom. If the tenant answers and wishes to admit the visitor, the tenant pushes a door release button on the video intercom in the office suite. The procedure releases the outer door only. Once the visitor is in the entry vestibule the concierge can then release the inner door. The system is designed to be fail secure, to compel the concierge to be present at all times to perform duties, to require dual control, and to involve tenants in the responsibility (and consequent liability) of persons they admit to the building.

Another problem arose with security in the entry vestibule. After hours the far right pair of lobby doors were to be used for exit and the far left doors for entry. The initial plan was to have a physical barrier built so that no one could cross from one side to the other. The ability to cross from left to right meant that a cunning criminal could time his or her entry to coincide with someone leaving and, cutting across the vestibule, enter the inner door before it closed.

The architect, however, vetoed installing any physical barrier. To compensate, we installed another curtain motion detector to electronically partition the left and right sides of the entry vestibule. Crossing the detection pattern created an alarm, which held the elevators on the lobby level. Therefore, no outsider could enter the building without going through a dual-control procedure, even if the person had a stolen access card and an accomplice inside.

An alarm system with central station monitoring and armed response was another feature of the system. All perimeter building doors were fitted with alarms as well as all interior fire stairwell doors. The concierge was given a wireless emergency button, a deadman's switch, and duress codes, which could be entered at the keyboard.

Communications to a primary central station were established via a standard alarm control panel with a built-in digital communicator over a telephone line protected by AA-derived channel service. Backed-up communications were provided via digital communicator and a long-range, AA radio to a back-up central station. Finally, an Interwatch radio was given to the concierge for direct voice communications to the local New York Police Department precinct.

Electronic locks were provided for all perimeter doors leading to the lobby and the street. The concierge was given limited control over these locks through the access control system, which logs all actions taken.

These locks were tied into the building fire alarm, which also provided the concierge with the only way he or she could override the access system. In case of a fire, medical emergency, or other critical occurrence, the concierge could hit the appropriate pair of twin emergency buttons on the desk. These buttons would activate a full emergency involving central station and police response. It would also recall the elevators and release both sets of entry doors.

The emergency buttons could not be activated by accident. They would require an adequate explanation for activation, and would cause a log to be created. To restore the system to a nonemergency condition would require an appropriate set of codes and functions to be entered on the system keyboard. Nothing the concierge could do would cancel the response to an emergency activation.

This system, like all systems, is far from perfect. A limited budget impeded the ability to control all fire tower doors with electronic locks. Therefore, nothing prevents someone already in the building from traveling to any floor via the stairwells. Although an alarm will be created by anyone opening a fire exit door, no security personnel will be on staff to investigate the breach.

Once inside the building no elevator control inhibits travel. A party can use the elevators to go to any floor. A camera is located in every elevator cab, but none is placed on any floor except the lobby, nor is there any access control on any floor.

No provision was made for outdoor protection either, and the building is abutted on many levels by adjoining buildings. The concierge belongs to a local union, so if there is a strike, the security of the building and its occupants could be impaired.

We did the best we could under the constraints we faced. We used resourcefulness and creativity to solve many problems. And we are certain we provided the owner with a far better level of security than he ever imagined. ■

Richard H. Cantor, CPP, is president of Amerigard Alarm & Security in New York City. This article is a Technology-at-Work Award winner.