

BUILDING OPERATING MANAGEMENT

Getting IN



Access control systems have become a jack-of-all-trades. Facility executives must ensure that the system selected, however versatile, still does Job One — keep intruders out

Taking a Balanced Approach

Improvements in technology have transformed access control systems. Today, an access control system is the backbone of many organizations' total security plan.

Not only does the access control system keep unauthorized visitors out of areas where they're not allowed, it also serves as the center for integration with other elements of a facility's security package, including CCTV, monitoring and alarm devices, security guards, and the facility's visitor management policy.

The increasing convergence of security, facilities and IT

has provided opportunities for other functions as well. Human resources may use the access control system to verify employee attendance. IT may use the system for logical access to computers. Access control systems can even affect how occupants pay for their lunches or control the temperature in their offices.

With all these factors to consider, facility executives designing an access control system face a challenge: maintaining the core goal of the system — ensuring a secure facil-

(Continued on page 48)

(Continued from page 38)

Balanced Approach

ity — while incorporating the peripheral features that will make other departments and end users happy as well.

The best place to start is identifying a facility's potential vulnerabilities, and then analyzing how the access control system will address those areas. Experts say that such an assessment usually begins at the perimeter — with parking lots or garages — and moves in concentric circles inward, to access points of the facility, to specific areas or zones inside the facility, and finally to particular devices.

If there are problems at any of those areas, analyzing how a specific system will address those problems is important as well. Once the vulnerable areas and problems have been identified, facility executives then can look at different access control solutions that will best mitigate those threats. For instance, if laptops have disappeared from a fourth-floor computer lab, the facility executive may want to examine an access control system that is integrated with a CCTV camera that switches on and sends video to a guard whenever the door to that lab is opened.

"The initial step is to conduct a needs analysis to define the goals that are to be achieved through the deployment

tion for security systems integration, the access control card is becoming the platform to securely identify a person to many other systems within the workplace environment," says Marc Freundlich, president of Indala. "Facility executives need to get the right parties around the table from the start, including human resources, security and IT. Roles must be determined and responsibilities defined."

Not only is soliciting other departments' input critical in determining the features of the access control system, it's also important for mapping out how the system will be deployed and administered. The more complicated the system, the more crucial the IT department is as an ally.

"More and more, access control and security products are becoming IT-centric," says Peterson. "Effective deployment now requires an increased level of technical expertise to effectively integrate access control devices and systems across an organization's network."

The access control system should be compatible with the existing IT setup and normal organizational opera-

Designing an access control system starts with IDENTIFYING A FACILITY'S POTENTIAL VULNERABILITIES

of an access control system," says Mark Peterson, director of the iTechnology design resource at HID. "The results of such an analysis will identify the desired aspects of an access control system from the perspective of each organizational element that may ultimately use, administer or support the system."

This means that the decision-makers from the key departments need to participate in determining how the system will function beyond just opening and closing doors. Those people will have input into what type of credentials — biometrics, PINs, magnetic strip cards, radio frequency identification cards (RFID) or contactless smart cards — the system will use and where access control devices will be placed. The type of credential chosen is also the vehicle by which other nonsecurity functions fit into the framework of the access control system. Certain types of cards can carry vast amounts of embedded information on a tiny chip, which allows occupants to use them for multiple functions all over the facility.

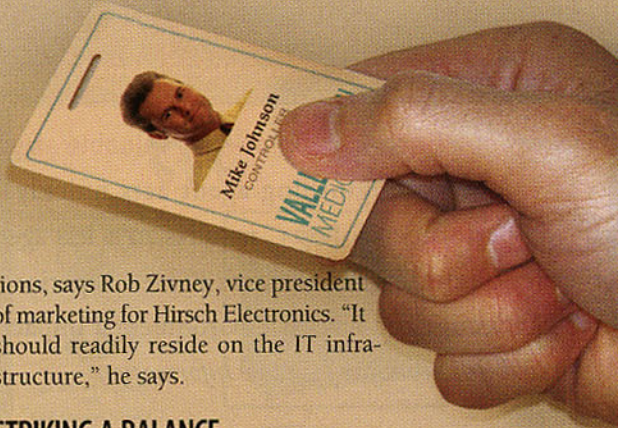
"Just as the access control system became the founda-

tions, says Rob Zivney, vice president of marketing for Hirsch Electronics. "It should readily reside on the IT infrastructure," he says.

STRIKING A BALANCE

Over-buying an access control system can be both expensive and problematic. For example, a complicated biometric access control system that takes several seconds for authentication may hold a certain amount of cachet for an organization, but it's probably not the best option at an office building's main entrance. Lines will form, people will get frustrated and chaos will ensue.

The key is finding the balance between an acceptable level of security and normal facility operations. "The facility still has to function even though access control has been implemented," says Bob McKee, director of business development at Pelco. "Improper design not accommodating for traffic flow during peak hours will cause tardiness and aggravation with employees who are attempting to abide by the security requirements."



'MUSTERING' GAINS POPULARITY AS WAY TO TRACK OCCUPANTS

When considering an access control system, facility executives often weigh its potential impact on occupant safety during an evacuation as well as its ability to prevent unauthorized entry. Can the system be set up so that certain doors are locked down by the access control system during an evacuation? And, if so, is there potential threat to the safety of those trying to evacuate? If certain doors aren't locked down during an evacuation, does a security threat exist? But even more importantly, is there a way to make sure everyone is present and accounted for after an evacuation?

LOGGING IN, LOGGING OUT

In facilities with high security requirements or where hazardous materials exist, the practice of mustering is becoming more commonplace. Mustering means using the access control system to keep a record of who is in the building at all times so that, in the event of an evacuation, a list of

everyone in the building at the time of the evacuation can be consulted and people checked off as they're accounted for. Essentially, the practice of mustering means that people log in and out of a building, just like they would a computer.

"Getting people out of a facility or campus is conceptually opposite to the primary function of an access control system," says Debra Spitler, president of Omnikey. "But it is an increasingly recognized and utilized function of access control systems. Most systems have this ability, yet it is underused."

To properly enact a mustering program, access control devices are installed at all exit points, or at muster stations — safety areas where people congregate in the event of an emergency. The visitor management policy must require card access and must be enforced meticulously, both by the guards and by the facility's occupants.

"If employees allow others to enter under their access control

card, or if a receptionist allows a vendor to deliver flowers to an employee's desk without signing in, or if a visitor is allowed to use the restroom for just a few minutes without logging the visit into the system, then the evacuation report is compromised," says Sheila Stromberg, access control manager for Fargo Electronics.

FURTHER PROGRESSION

As mustering becomes a more popular method of using access control to keep track of building occupants' whereabouts, facility executives will discover other ways of using the strategy.

One natural progression of mustering is strategically placing access control devices at doors so that different facility zones are created. With that approach, it would be possible to tell approximately where in the building a person is at any given time, or if the person is in the building at all. CCTV cameras could then help pinpoint the person's exact location.

—Greg Zimmerman,
managing editor

Even if the design of an access control system perfectly matches the security and operational needs of a facility, there's always the danger that elements of the system will be neglected either because they're improperly integrated into the total facility security plan or because facility executives don't take the time to learn how to use them. This means that the system isn't operating as designed and could lead the facility executive and the occupants to believe that they are safer than they might actually be.

While over-blowing and then under-using an access control system can be costly, under-designing one can be even worse. If upper management is unwilling to invest the necessary capital to fully fund a proposed project, facility executives should provide return on investment details about what a breach in security might cost the organization if an occupant were to sue. The facility executive can also provide data to show how an access control system can save money long-term by reducing stolen property.

But if the capital really isn't available, skimping on the system may be worse than doing nothing at all. "If misapplied, access control can lead to a false sense of security,"

says Tony Padilla, chief technology officer for Stanley Security Solutions.

FLEXIBILITY IS A PRIORITY

Even if the access control system is working perfectly for the current security situation, it should still be designed so that it's scalable to address future needs.

"The built-in scalability of many of today's access control technologies provides a migration path that allows an organization to add features and expand the system as budgets allows," says Holly Sacks, vice president of marketing for HID. "Facility executives can make technology choices based on what they need today and what they will need in the future, rather than simply on what is available."

The system should also be flexible to handle changes in the security situation or threat level. This may include everything from the national color-coded terrorism threat level to switching the number of credentials needed to enter after 5 p.m. Many access control options exist that would require only a card swipe under ordinary circumstances. But if the situation changes, the device would