

Improve Facility Security

10 tips that building managers or security directors can implement today to assure a facility's security/access control operations remain cutting edge for tomorrow.

- 1. Modify for a Lock Down.** Many facility managers want the expediency of locking down a building with the activation of one button. If a major city is hit with a dirty bomb, for example, a hospital must have the capability of locking down all access doors immediately to minimize interior contamination by panicked incoming infected victims. However a mechanism to allow first responders is needed
- 2. Prepare for Disaster Recovery.** If IT department's server room fails, will the facility's access control/security systems that are tied into it still operate? Unless there are accommodations for fault tolerance where the database server or building controllers fail-over to an unattended alternate, which could be (and should be) hundreds or thousands of miles away, the access control/security system is susceptible to disasters such as fire, earthquakes, hurricanes and other disasters.
- 3. Plan a Five and 10-Year Security Mission.** Surprisingly, many facilities don't have a five and 10-year plan, but the security department should have them. Today's facility's access control/security budget may not parallel a planned increase in planned physical building personnel additions.
- 4. Preparing to Remain Cutting Edge Tomorrow.** Will a building's current access control/security software easily accept tomorrow's technology? For example, in the next five years facial recognition could become a standard. Beyond that, video analytics will determine someday whether an assault is actually taking place simply by detecting body motion through a set of algorithms.
- 5. Use Subtle Barriers to Protect Areas.** How a security or receptionist area is viewed by perpetrators can thwart breaching attempts. For example, an elevated receptionist desk area with high profile counters, which is commonly used in bank teller areas, can subconsciously and physically challenge someone from jumping over and breaching a secured area. Building an effective barrier without a jail-like appearance is a delicate balance.
- 6. Continually Updating with Hardware/Software Upgrades.** If a facility's security requirements aren't growing, then the security threat exposure is also growing. An access control/security system must have the capability to be upgraded so the latest tools are available to security personnel such as guard tour, ADA, hot failover door controllers, vectored graphic floor plans, flow control and advanced reporting.

7. **Request a Security Review.** A review by a consultant can surface many weaknesses in a building's overall access control and security that aren't apparent to the facility's security staff. Some manufacturers offer free consulting services to customers or charge a fee that is refunded if the consultation results in a contract.

8. **Use Subsystem Gateways For Remote Locations.** Remote locations such as doctor offices, storage buildings and parking lots can be secured cost-effectively with subsystem gateways, which use an IP network to extend a main facility's security systems to isolated areas without full-fledged equipment/personnel set-ups.

9. **Increase Badge Security.** Increase badge production usability by incorporating photos, different background colors for levels of security, and counterfeit-proof microprint authentication or RFID technology that's embedded in the laminate coating or card stock itself.

10. **Add Another Security Level to Access Control.** If access is only through a magnetic stripe or proximity chip on an ID badge, then add readers that will also use PIN touch pads for an extra level of security in ultra-sensitive areas or during less usage times. Biometrics -- using fingerprint, iris or facial recognition -- can be yet another level.