

Campus Security Update

Integrated approach in action

TALK TO campus security administrators these days and you will find securing the premises—whether a research lab at Johns Hopkins or a sorority house at Chico State—at the forefront of their planning.

“Securing a campus as large as the University of South Florida (USF) is no easy task,” said Adrian Cuarta, director of the Physical Plant for the campus. “With 35 large buildings that require access control, thousands of users who need access after hours and more than 800 doors to lock, simply locking and unlocking doors every day was a logistical nightmare. We wanted all the buildings to be locked at 10 p.m. but the process could take until 3 a.m.”

Lessons on integration

Locking buildings was intermittent at best, he said, until recently, when USF upgraded to an access control and security management software system that automatically locks campus buildings on a set, predetermined schedule. The system was integrated with existing magnetic stripe-based card readers, a closed-circuit television surveillance (CCTV) system, fiber network backbone and databases.

The campus now has one integrated access control system for 5 million square feet, including 829 doors, 205 card readers and 148 cameras. Approximately 8,000 users have been entered in the system.

“In an emergency, we can now lock the buildings at once. The most recent hurricanes have gotten pretty close and if we want to lock the campus down in the middle of the day because of an evacuation order, it’s now possible to do that,” Cuarta said.

At Johnson & Wales University in Denver, officials went one step further, implementing biometrics.

“Only biometric solutions can verify a human being,” said Lindsay Morgan of the university’s media relations department. “It allows authorized individuals

to access an area and keeps everyone else out. Students don’t have to worry about an unauthorized individual picking up a lost access card, or students loaning out their cards to strangers.”

Readers are located at the main entrance of residence halls, requiring students entering to slide their hands onto the device. They are admitted in less than one second. They follow the same procedure when they arrive on their floor and at their residence.

From a management standpoint, officials can retrieve reports on building access, assess traffic patterns, investigate unauthorized events and record activities. Doors can be unlocked remotely and a special code alerts campus safety officials in the event of an emergency.

At the University of Central Florida in Orlando, biometric technology is employed to heighten security at two sorority houses.

“Both houses were experiencing problems with unauthorized students at all hours,” said Bill Spence, biometric business manager, Ingersoll Rand Security Technologies, Campbell, Calif. “To prevent those occurrences, the readers employ redundant access to the sororities. Each student must enter a PIN code and present their hand to gain entry.”

Ara Bagdasarian, president of Omni-Lert Inc., Leesburg, Va., produces a software program that is a one-way messaging system that all but eliminates sirens, intercom alerts and telephone trees.

Students, he said, now come to school equipped with cellular phones, so the use of a dormitory’s hard-wired telephone system is outdated.

“So the challenge becomes finding methods of contacting them, even when

they are off campus,” Bagdasarian said, for alerts that may be as routine as a weather alert, or as threatening as a hoodlum running amuck on the campus.

“Messages may be sent to cell phone numbers, pagers, via e-mail, via voice mail or to PDAs. Anyone owning any of these devices who can figure out how to turn it on will be in the communications loop,” he said.

Identification cards and readers are not a thing of the past; they now have increased capabilities instead. Multitechnology readers can be used for a host of vendors and security activities in both contact (swipe) and contactless (proximity) smart card versions.

How to select

“Whether smart cards are used now or will be implemented in the future, it’s important users are not tied to one format only,” said Steve Waylin, GE Security’s director of product development, Engineered Systems, Boca Raton, Fla.

“We help them establish a flexible, scalable, non-proprietary framework that lets organizations maintain their current user bases, yet upgrade their access control systems to meet new security requirements on their own timelines within budget.”

GE’s readers allow companies to continue using their existing proximity cards when migrating to even more secure systems. They also permit multinational organizations that use a variety of legacy credentials to access facilities company-wide.

Considering their population and characteristics, college campuses are beginning to look more like small cities. As a consequence, the same technology designed to thwart terrorists is becoming the standard campus security is measured against. ■

LAWRENCE is a freelance writer and photographer based in Bozeman, Mont. He can be reached at hsrcrk@mcn.net.