SECURITY MANAGEMENT
JULY 2007

Case Study

BY TERESA ANDERSON

Campus Access Controlled

In need of an access control system, security at the University of Pittsburgh sought a solution that would support existing ID cards.

WHEN JOSHUA COCHRAN, manager of integrated security for the University of Pittsburgh Police Department, went shopping for an access control and alarm system, he had already laid the groundwork. He had established a computer network and installed electronic key locks on the perimeters of campus buildings. What he needed was access control hardware and software that could be integrated into the existing system.

The University of Pittsburgh, founded in 1787, consists of 68 buildings on 132 acres in southwestern Pennsylvania. More than 11,000 employees and about 25,000 students work and study there.

Though the police department had always been tasked with keeping the peace on campus, Cochran took on access control duties from the operations department several years ago. After the change, he set about replacing old mechanical locks with new electronic keypad locking units and establishing the computer network, independent of the university's network, for security-related systems.

Two years ago, when he was ready to purchase an access control system, he had two requirements. First, the access control system must have a hardware base that was compatible with the Mercury Systems hardware that Cochran was already using for the locking devices. "Part of our research process was to find a software application that could use the hardware that we had already invested in," says Cochran.

Second, the software had to have the ability to interface with the university's existing ID cards, which were also used to store funds for meal plans, to serve as ATM cards, and as a library card.

For advice, Cochran turned to the Pittsburgh Steelers football team, which he knew had recently installed a security system. Both the Steelers and the Pitt Panthers play their home games at Heinz Field in downtown Pittsburgh. Senior management from the Steelers put Cochran in touch with a security consultant. The consultant, in turn, suggested several product manufacturers.

Cochran narrowed it down to two possible vendors. "The biggest variable was their ability to interface with our system," says Cochran. "One company was willing to spend a lot of time with us exploring what our needs were and then rewriting their program to meet those needs."

That company, RS2 Technologies, LLC, of Munster, Indiana, used Mercury hardware for its backbone system, including the card readers so it could interface with the existing mechanical locks. The company then rewrote its Access It Enterprise software, which was designed for campus and multibuilding environments so that it would work with the university's existing ID cards.

PHOTO © CIDDE/UNIVERSITY OF PITTSBURGH

The existing computer network had been built internally by the university. However, RS2 helped build a redundant server system to ensure that the access control system would work in the event of a power failure. This was a crucial step, accordingto Cochran.

"It was critical that we have a network infrastructure to run independently of the university network and purchase a server backbone to have redundancy and reliability," says Cochran. "We didn't want to have the problem of relying on the university network."

Installation of the card readers and software was completed with the help of RS2 personnel, along with a four-person team from the university police department. Cochran also contracted with an electrician to be on hand during the installation process.

The first access control points were installed in a dorm and a research lab—both under construction at the time. That was two years ago, and Cochran has been expanding the system to additional buildings ever since.

> "Any device that can send a signal, we have been able to tie into the system."

Currently, almost 40 buildings have been fitted with the system including several dorms, all of the campus research buildings, offices, sports facilities, and retail stores owned by the university. Cochran is in the process of converting 30 additional buildings—some off-site—to the new system.

Cochran was so pleased with the access control system that he expanded the enterprise software to control other devices. "We have door alarms, glass-break alarms, burglar alarms, and panic buttons," says Cochran. "Any device that can send a signal, we have been able to tie into the system."

For example, the software is also used to monitor keypads used on interior rooms, such as office suites and multimedia centers. Similarly, the software monitors wireless receivers for the university's perimeter security system, which includes automated gates and bollards.

Cochran is pleased with both the system and the university's integrated security stance. "This approach is not only safer, it is also more convenient for us to have one card and more comprehensive reports," says Cochran. "The departments, staff members, and students also benefit. And, in light of recent incidents like the Virginia Tech shooting, the system has more than paid for itself in peace of mind." ■

(For more information: Dave Barnard, director of dealer development, RS2 Technologies; phone: 219/836-9002, ext. 225; fax: 219/836-9102; e-mail: dbarnard@rs2tech.com)

Teresa Anderson is senior editor for *Security Management*.