Security

Technology Applications for End-User & Integrator Buyers

Conventional WISDOM

By Steven Rindner, Contributing Writer

Last summer, parts of New York City resembled an occupied territory. As the 2004 Republican National Convention rolled into town, numerous Manhattan residents took off work and left the city for the duration, fearing both traffic backlogs and potential protestor or even terrorist violence. At the epicenter: Madison Square Garden.

So it may come as a surprise that at 11 Penn Plaza, right in the Garden's backyard, the building's tenants and visitors experienced, well, virtually nothing out of the ordinary. No security breeches, no threats; not even excessive noise was reported during the convention – quite an accomplishment considering the expected ruckus.

Party at the neighbors

In the months leading up to the convention, higher security standards were suggested for buildings in the Penn Station submarket. Tenants of the 1.1 million square foot property had also expressed concern for their personal safety – and Vornado Realty Trust, the owner and manager of 11 Penn Plaza, didn't want its tenants to fret.

As one of the largest real estate investment trusts in the United States, Vornado was no stranger to the need for superior and cost-effective security – but the time constraints imposed by the imminent convention were unusual. Under ideal circumstances, the trust would usually take a year to coordinate and manage the various elements of such a security solution. With much shorter notice before the GOP showed up next door, they would need to hire consultants to design a system, select and negotiate with a vendor to install it, train building engineers to operate it, instruct security personnel to monitor it, train office personnel to administer it, educate tenants to use it, and make provisions for ongoing programming, changes/upgrades and maintenance to ensure the functionality of the system over time. Each task had potential hazards, and the trust had a small window of time within which to execute them all.

The trust determined that dealing with multiple parties was not feasible; they needed a single point of execution to be responsible for all functions. What they found was Washington, D.C.-based Kastle Systems, with electronic access control and building security as their specialty.

Uncovering problems

Known for its diverse and unique operations, the trust was not satisfied with the system in place, as a security system audit uncovered several problems with the existing access control system.

Access controls were upgraded including real-time administration of cards into the property through Kastle Systems.

The 11 Penn Plaza in New York City sought one source help when facing last year's Republican National Convention in the neighborhood.

The card reader for tenant admission was not a proper deterrent to unauthorized users. Access card activation and administration for tenant employees lagged employee rosters. Activity reports were difficult to generate. Technical support for tenants was slow. Tenants, building employees and security guards were frustrated by the inefficiencies of the system and were abandoning the existing access control system all together.

The underlying problem was one that many building owners and managers experience: the existing system, while only several years old, was inflexible to upgrades and caused even the most basic elements of the system to perform poorly.

A thorough threat analysis was performed to determine optimal security system design for the building. With input from Vornado management, building employees and tenants, a comprehensive security solution that incorporated components of the original system was installed and operational in just three weeks.

The security service contracted by Vornado includes remote monitoring of a diversity of systems to support the building's owner and manager.

The security company upgraded 11 Penn Plaza's existing access control by adding prop points to monitor doors to the freight loading dock and installing an audible panel. Panel monitors would control tenant admission by reading cards instantly and emitting a signal to alert guards when it detected an invalid card. To ensure access cards could be activated/deactivated in real-time, Kastle enabled card administration and reporting through the Internet, making it accessible from any location. All building information was contained in a database backed up in multiple locations and controlled by the company.

Additionally, the trust's building security personnel were introduced to the new system and trained to operate it properly. Tenant confidence was restored through proper education of how to use the system to ensure optimal security.

Continuing relationship

As the Republican Convention came and went off without a hitch, the company's work had just begun, as the company considered the process of securing a building as ongoing. The security company's trained staff of professionals are now responsible for monitoring all building alarm points, and the status of interior and perimeter building doors, as well as conditions such as temperature, flood, smoke and equipment failure. They are also responsible for running the system to ensure performance, managing and operating redundant telephones, computers, software and manpower, and backing-up the system. Programming responsibilities involve implementing all changes to the operating system – for example, incorporating tailored response procedures, exception events, and out-of-the-ordinary protocols – and updating hardware and software. ❖

About the Author

Steven Rindner is with Kastle Systems with headquarters in Washington, D.C.