Is Our Telecommunications Infrastructure Secure?

High-tech options can help solve industry's unique problems

By Andy Hilverda

The events of Sept. 11, 2001, and the 2005 hurricane season emphasized U.S. dependence on an effective national telecommunications infrastructure. Telecommunication companies are a critical part of America's infrastructure and key to securing the homeland in times of emergency. Reliable, resilient communication services can provide the bridge between emergency responders, firefighters and law enforcement for cohesive emergency management.

Security is paramount to the telecommunications industry, but companies face unique challenges in implementation because of the way they are structured. Companies must secure their networks while managing hundreds of properties over geographically widespread regions. Understanding who has access rights and when they exercise those rights is essential to securing operations.

Unmatched Challenges

The ongoing problems in managing remote, isolated sites are more related to vandalism and theft than terrorism. With the tremendous increase in the price of copper and other metals, substations and equipment rooms have become prime targets for thieves. Keys are being duplicated, and companies have no idea how many keys they have out in the field. Thieves gain access to equipment rooms to steal expensive network switches so they can sell them outside the United States. Cabling is stripped for metals and sold on the open market.

There also are serious access control issues for owners of rooftop antenna-site equipment rooms with multiple, co-located wireless carriers sharing the different subdivisions within a room. All have their own technicians coming and going. Maintenance people for the building's physical plant also need access rights.

In some situations, there may be a CCTV system in place, or independent security cameras at the entrance to the building. However, in most cases, no system has been implemented for identifying who is accessing the different subdivisions within the equipment room. Owners have no idea how many "lost or missing" keys are still out in the field or how many keys are being used for criminal purposes.

Remote cell tower sites face similar problems, but their vulnerability is heightened by their isolation. Once again, owners often have no system in place for tracking the cell and switch technicians who visit their sites and have no level of control over the keys issued. Another concern is that most sites include a padlock on the gate, one or two doors on the equipment room and a door to the structure that houses the generator. Often, each type of door hardware and padlock is of a different make and manufacturer, which only compounds the problem of key control.

These are some of the troubling problems that confront companies in developing a strategy for securing their sites. As companies begin to tackle these issues, they look for an access control system that offers high security and flexibility. Most importantly, they look for key control and an audit trail. Because they face an overwhelming array of choices, costs and undefined benefits, companies need to have a methodology in place for pursuing a balanced approach to their security goals and a way of measuring the success of their efforts.

A security plan must be scalable to allow telecom companies to control access to multiple facilities and track multiple identities. Touching on some solutions that are available today, here is an overview of technology that might be considered for integrating into an effective plan to manage site security.

High-tech Options

Entry door systems are available that use biometrics for either authentication or identification. Until recently, large biometric applications have been impractical because of the cost of replacement hardware and installation. And, a huge amount of memory is required to store biometric templates.

Biometric technology is evolving with a wide array of new products for single door and stand-alone solutions. However, this technology needs to consistently provide higher performance in products designed for commercial applications.

Multilocation digital video security systems are a viable option for surveillance of rooftop antenna-site equipment rooms. As the technology has evolved, cameras have become more compact and now are able to produce images under limited-light conditions. There are a host of products to choose from, and the task of researching choices may be daunting—but they are certainly worth looking into.

When considering digital video, be aware that there are limitations to bandwidth size, and video files are often extremely large. Bandwidth and file size are closely related. Digital signals of the images need to be processed and transmitted over a network in a reasonable length of time. The larger the video image, the larger the bandwidth needed to transmit the image over the network. When hundreds of cameras are installed over a large geographic area, compromises usually have to be made as to the level of image quality and the frequency of reproduced images.

Emerging technology is bringing IP-based security solutions for networked environments to provide collective surveillance, access control and identity management to large organizations. This convergent technology incorporates IP cameras, IP video servers, video analytics and security-explicit storage solutions. IP security should be researched thoroughly to determine the cost of all the elements, including installation. Are there dedicated funds for the installation? Have administrative costs been considered to efficiently manage the system after installation? Is it the correct technology for the immediate problems?

Advances in technology have brought us wireless video verification. These systems combine battery-powered cameras, sensors and GPRS communication with a central monitoring station. Video-verified intrusion alarms are becoming more practical as the costs of CCTV decline, making them a more practical solution for locally based security. Telecom site owners can benefit from a wireless system when there is an intrusion, quickly determining whether the intrusion is nonthreatening or more serious.

Key Control Issues

If key control and an audit trail are the immediate concerns of most telecom companies, what's available to get control of the keys? How can they control and audit the comings and goings of subcontractors and technicians who visit their sites?

"In working with telecom companies, I see a hodgepodge of all types of padlocks, door hardware and keys," said John Switzer, owner of Trevino Lock and Key in El Paso, Texas. "Nothing is keyed the same, and they have no way of quantifying their security risks because of the unknown number of keys in circulation. Companies gain control over their keys and have an efficient method of tracking their technicians and subcontractors with the CyberLock® electronic lock system."

This system is unique in that it incorporates the mechanical lock hardware and padlocks already present at telecom sites. The mechanical cylinders inside existing locks are replaced with electronic cylinders, all without hardwiring. The locks and keys store an extensive audit trail so owners can know when vendors visit their sites.

Verizon Wireless has implemented the electronic lock system throughout its facilities.

"We wanted better control over who entered our buildings and a system that would allow us to track key usage," said Jackie Johnson, manager of operations for Verizon Wireless in the Carolinas. "With the electronic lock system, we have achieved that. Now we can track vendors completing services and other functions."

A subcontractor's key can be programmed to open multiple locks and padlocks. In addition, a key can be set with a period of time it will function before it becomes inactive. The electronic lock system supports a variety of methods for communication between the hardware and software, including the use of cellular PDAs to program keys on demand in the field.

All of the solutions mentioned are certainly very capable and can be integrated into a cohesive plan for meeting telecommunications' ever-widening security concerns. With today's advances in security technology, organizations have the opportunity to implement integrated systems that provide physical security, accountability, and, most importantly, key control. ✯

***Andy Hilverda** is vice president of Videx Inc.*