Brave New World: Integrating electronics into a hospital security plan

By Bill Van Vlack, P.E. LEED®AP and Tony York, CPP, CHPA

(published in *Health Facilities Management*, November 2006)

The threat of terrorist attacks, an increase in weapons being brought into health care facilities, possible occurrences of infant abductions, and data security requirements of the Health Insurance Portability and Accountability Act (HIPAA) are keeping all eyes on the effectiveness of security programs in hospitals.

Thus, it is not surprising that more health care organizations are looking to supplement their existing programs with electronic security systems. And increasingly, electronic security systems are converting from analog to digital, Internet protocol (IP)-based equipment to provide and transport information that hospital staff need to manage security threats.

With more systems capable of running over the facility's cabling infrastructure and data network than ever before, there are new opportunities for integrating and converging these systems into a hospital's overall security program. Drawing on these opportunities creates new challenges for staff with security responsibilities.

**State of security**

Moving away from the reactive approach of the past, many health care organizations are implementing security plans that target their patient populations and specific building needs. Risk assessment programs such as the CAP Index CrimeCast Map and Site Data (http://capindex.com) are designed to help hospitals analyze the demographics of their city and pinpoint risk. Coupled with the services of a competent and credentialed health care security professional, these organizations are better equipped to manage their real and perceived security risks while balancing the customer-oriented needs of a healing environment.

An innovative development in electronic security design that supports these plans and programs involves using a facility's cabling infrastructure and transmission control protocol/Internet protocol (TCP/IP) network to stream images from closed-circuit television (CCTV) systems to digital video recorders and monitors. Such an infrastructure can also be used to transport access control information between data servers, panels and workstations.

The structured cabling system includes copper unshielded twisted pair horizontal cabling (Category 5E or better) that connects electronic security support system components to the nearby telecom closet, and optical fiber backbone cabling that connects data switches in the building closets to routers in the main IT equipment room. The cabling, switches and routers make up the IT infrastructure (data network) of the building that transports IP packets of information between devices.

With the increased flexibility of the data network comes the associated risk of bandwidth contention with the new digital-based cameras. While approximately 90 percent of cameras that are currently installed in hospitals are analog-based, the leading manufacturers of CCTV cameras have released IP network-based digital cameras, and hospitals are starting to include them in their planning, strategic direction and standards development. Facilities must make sure their network employs the specialized requirements for the high-bandwidth optical fiber backbone cabling and enhanced data switches that serve these cameras.
Depending on the system, connecting cameras to the network could mean significant changes to the hospital's information technology networking hardware. For example, routers and switches are now being provisioned with multicast and quality-of-service features. If a facility is adding cameras, it's important to consider whether the cameras will be placed on the hospital data network or on a separate stand-alone network that consists of backbone cabling, data switching and routing equipment.

New skills and training are necessary to facilitate this level of decision-making. Traditionally, analog security systems were maintained by the security department, physical plant or facilities staff. The information technology department was tasked with long-range planning, set up and maintenance of the hospital's data network.

As the IP data network becomes the system of choice for transporting information between real-time systems, such as access control, video, infant security and even voice panic systems, information technology staff is becoming increasingly responsible for maintaining and operating the data component of these systems.

In many hospital organizations, the chief information officer is now responsible for both building and data security, while other hospitals are choosing to keep building security separate as a core competency within the facilities department.

**Implementation tips**

In either case, implementation of new or upgraded security technologies requires the same basic groundwork. The following tips will help health care facilities ensure a more secure environment:

- Engage the hospital’s IT staff early and often to ensure that the cabling, networking and software support resources are available and reliable as the plan is implemented and used in real-life situations.
- Ensure that adequate space, reliable electrical power and sufficient cooling is provided for each component of the electronic security support system.
- Clearly delineate in the hospital’s strategic plan whether the security or nursing staff has authority for intervention, particularly in the ED and other volatile areas.
- Maintain thorough records of electronic security system components, including component labeling, location, cabling types, cable termination information, equipment cut sheets, node and port IDs, application software routines and IP addressing and network configuration information.
- Engage in ongoing training on new systems.
- Consider employing the services of a security professional to provide detailed reports, attend security seminars and training programs, research specific areas of risk and advise on purchasing. To share the cost of this service, it is common for two or more facilities to develop a joint security program.

Working together, hospital departments can make patient and staff security a top priority. This is especially true for areas of high risk, such as the hospital's perimeter, emergency department and infant/pediatric care areas.

**Perimeter access control**

Building perimeter systems include life safety and emergency communications, with consideration of employee as well as public entrances.

Section EC 1.2 of the Joint Commission on Accreditation of Healthcare Organizations compliance manual requires that hospitals "have a plan to control ingress and egress from each defined Security..."
Sensitive Area." Based on the risk, this plan could include the use of electronic access control or screening personnel, appropriate signage and/or staff monitoring.

After-hours continues to be the primary time of risk in health care facilities. Having a single clearance point to areas such as the ED is recommended to control access at night and is an opportunity to integrate customer service staff with security efforts.

Lockdowns of the ED or the entire hospital are becoming more common to protect patients and staff. A two-stage process can facilitate crowd control during a lockdown, as follows:

**Stage 1.** Specific entry/exit points are locked and a physical presence (such as a security officer) may be required.

**Stage 2.** All perimeter doors are locked or staffed.

Electronic access control systems are increasingly used for these functions, with wireless or hardwired duress and lockdown buttons provided for key personnel to close and lock Stage 1 and Stage 2 doors.

Strategically placed card readers, along with system programming, can restrict passage through the doors to security personnel only during lockdowns. Strategically placed cameras with on-board or server-based motion detection can be integrated with the access control system to provide alarm notification, response and logging at a central monitoring location for remote perimeter doors and vulnerable areas.

**ED considerations**

A four-year study conducted by Henry Ford Medical Center in Detroit reported that 4 percent of persons arriving at the emergency department carry weapons. An increase in the use of illegal drugs, language barriers and illiteracy, and family issues such as estranged spouses, custody disputes and abusive relationships, create great potential for volatile situations to erupt in the emergency department.

In response, the American Medical Association, the Emergency Nurses Association and the International Association for Healthcare Security & Safety have promoted and enacted resolutions for increased security in the ED. The American College of Emergency Physicians also has ramped up its research and education efforts to provide a safer environment for patients and health care professionals.

One industry-recognized best practice for emergency department security is to physically separate the walk-in/reception space from triage and treatment areas and patient "quiet/safe rooms," and to control access to these high-risk areas.

Properly designed patient registration desks, triage areas and cashier stations can do double duty as service-oriented barriers in the ED. It is also helpful to have a designated entrance to control access to patient areas after visiting hours. To minimize staff inconvenience, a single clearance point with a camera, intercom, monitor and remote door release system is recommended. Modern access control systems connect via an IP network to an access control system data server, which provides information to client workstations where staff can issue visitor badges, respond to alarms and operate doors. Interfaces to pagers, wireless phones and wireless e-mail or Web page display devices are common in higher-end access control to provide security alarm response systems. The security office and dispatch center is often located in or near the ED.

Other security measures might include CCTV camera systems at the walk-in/reception space and waiting room for post-incident investigative purposes, at each entry/exit for control of access to the department and in observation rooms for remote monitoring of patient safety. Metal detectors at the ambulatory and ambulance entrances, card access equipment and panic
duress alarms at the walk in/reception desk and at the triage and nurses' station may also be recommended.

With digital, IP-based CCTV systems, camera images are now available anywhere the data network is available, unlike analog systems that generally require coaxial cable at each viewing station. Where HIPAA is not a consideration, images generated for security operations can also be utilized by staff or the public.

Digital video recorders (analog cameras) and network video recorders (IP-based cameras) are often used for forensic analysis of events. These products offer advanced video processing modules that can be applied in a hospital setting, including face and object recognition and crowd anomalies (e.g., someone leaving an object such as a backpack, people traveling the wrong direction and motion detection). A recent trend is that the cameras themselves have video processors, which can reduce network bandwidth requirement by sending high-speed, high-resolution images over the network only when required.

Depending on the size of the facility, a roving security officer might be adequate; however, a 24-hour staffed ED security post is often required in trauma-designated facilities.

**Infant/pediatric areas**

Due to education and training efforts of the National Center for Missing & Exploited Children and other organizations, the number of infant abductions has decreased dramatically. The use of CCTV, electronic access control and infant protection systems, in conjunction with staff training, parental education and a critical incident response plan, have been instrumental in this effort.

Electronic infant protection systems range from basic systems that sound an alarm when an infant is taken into certain areas to computer-based systems that identify and track infants, lock doors and elevators and provide timed alarm activation. Challenges of installing these systems may include differentiating portal and tamper alarms, properly testing the system and managing nuisance alarms. Hospitals are increasingly integrating electronic infant security systems with access control and CCTV systems.

CCTV systems should provide a face shot of all persons leaving the birthing unit, with cameras placed at the main corridor entry, at each exit point and at each elevator. These cameras should be tested every 30 days. Camera maintenance is an area where IT and facilities professionals are collaborating and cross-training, particularly with the introduction of IP cameras in the health care environment.

Higher-end access control systems feature door release and camera monitoring in infant/newborn areas and are often attached and integrated with partitioned access control system workstations rather than stand-alone controls and monitors.

To control access in birthing areas and nurseries, staff members who work in these areas should wear identification that is unique from regular hospital staff badges. Temporary badges can be issued to students or staff who visit the ward; however, a process of storing, retrieving and destroying these badges is hard to enforce. In addition, nurseries, employee lounges and locker rooms should remain locked at all times.

Electronic access control systems can fulfill these requirements with the use of temporary proximity-based badges that allow only authorized personnel to enter sensitive areas and automatically disable student or staff badges after a certain length of time. When badge production software and printers are integrated with the access control system, unique access control badges can be produced to visually and electronically identify personnel.

**The ideal system**

The ideal hospital security system is a combination of the right technology, careful planning and a strategically deployed staff. When these elements are properly integrated, the hospital is able to provide a
safe environment, and its employees are consequently able to concentrate on fulfilling the hospital's overall mission of providing high-quality patient care to the surrounding community.

Bill Van Vlack, P.E., LEED AP, is an associate at Sparling, a Seattle-based electrical and technology consulting firm for health care planning and design. He can be reached at bvanvlack@sparling.com. Tony York, CPP, CHPA, is senior vice president-security at HSS (Hospital Shared Services), Denver, which provides security management services and system integration solutions to hospitals and other health care facilities. He is also president-elect of the International Association for Healthcare Security & Safety. York can be reached at tyork@hss-us.com.