High-Tech Sentinels:  
The role of equipment in an overall security effort

By Tom Leonidas, Jr., P.E. and Jim O'Donnell

(published in Health Facilities Management, July 2005)

Hospital security is often overlooked or insufficiently addressed during the planning and design phase of a health care construction project; yet hospitals face security threats on many levels and security must address many aspects of a hospital including patients, staff, visitors, buildings and grounds.

Many hospitals install stand-alone systems for infant security, perimeter access and closed-circuit television. These are steps in the right direction, but by stepping back from the individual systems and taking a more global look, it is possible to design and install security systems that are scalable, integrated and that enhance the security environment.

Such efforts can reduce costs and mitigate exposure to criminal activity, allowing caregivers to focus on helping patients heal.

Determining threats

The first step in planning any security design is to perform a Vulnerability and Risk Assessment (VRA). The VRA allows the hospital to determine the potential threats in the hospital environment. Threats to a hospital may include the following:

- Physical threats to staff, patients and personal security;
- Theft of drugs or personal belongings by both staff and nonstaff;
- Kidnapping of infants and children;
- Communications failures;
- Theft of information and intrusion into secure data systems;
- Equipment theft;
- Arson, sabotage and general vandalism;
- Critical equipment failures;
- Natural disasters, such as floods and earthquakes; and
- Terrorism and bioterrorism.

The VRA begins by retaining a qualified security consultant with a strong track record of threat analysis, specifically in health care facilities. The assessment team then takes a layered approach that looks at physical security, information security, existing hospital policies and potential threats to the environment, patients and staff.

The mission of the VRA is to ferret out the weak links in the overall hospital security. Once they are identified, the hospital can apply the right security technologies and policies. This also ensures compliance with Joint Commission on Accreditation of Healthcare Organizations (JCAHO) requirements, which call for annual security self-assessments, especially for infants.

The VRA looks at every aspect of the facility’s operations, staff, patients and physical environment. It asks critical questions in several areas, including the following:

- Surrounding environment. What are the characteristics of the surrounding environment of the hospital? What are the risk factors from the outside environment? What are the recent security and criminal breaches reported within the local geographic area?

- Building and campus access. What are the sensitive areas within the hospital
and campus and how is access controlled? How do visitors enter and exit the facility? How is it monitored? How are locations of the building’s main infrastructure accessed and controlled?

One of the most security-sensitive areas is the ED because it funnels people into the hospital 24 hours a day. Because people with behavioral issues or people looking for drugs are drawn to the ED, hospital staff should make it a top priority for protection and monitoring.

- **Personal security.** How are patients protected from potential harm from outsiders or insiders, including physical harm and sexual crimes? How is staff protected from disgruntled patients and verbal abuse?

- **Identification.** How are staff clearly identified? How are patients clearly identified? How is access to security clearances, staff uniforms and other identifiers reliably achieved?

- **Bioterrorism.** What are the sensitive areas of the building for possible bioterrorist activity, such as location of fresh air intakes for fan systems?

- **Information theft and data security.** How much information does a hospital inadvertently expose to the public? How is information protected from unwanted predators from both outside and within the hospital?

- **Practices.** What policies and procedures are in place for handling breaches of security, theft and life-threatening issues as well as verbal aggression from patients and visitors? Is there ongoing training for staff about how to respond to security threats?

- **Security administration.** What is the dependency on and efficacy of electronic surveillance versus roving security guards, or both? Are the security systems and procedures seamless between multisite/campus hospitals?

- **Theft.** How are drugs accessed and controlled? How are patients' belongings protected from outsiders and staff? How is medical equipment tracked? How is theft of computers and sensitive patient information prevented? How is identity theft protected against?

It is critical that the VRA step not be taken lightly because it is the very foundation for the ultimate plan and systems that are implemented. Once the assessment is made through the VRA, it is documented in a Vulnerability and Risk Assessment Report that addresses each perceived risk and how it might be handled in a security plan.

The strategy for the facility's security plan and measures should evolve around a combination of security equipment, a security force and guards, training and security procedures. The strategy, much like the VRA, is a multilayered approach that addresses each element of risk.

When planning security, one should think of establishing three concentric protection rings or layers. The first layer is the perimeter of the campus — monitoring and controlling how people get in and out of the campus. The second layer is the actual buildings on campus. The third layer is sensitive areas within the buildings or the campus that need protection. Once the layers are clearly defined, there are a number of elements to the security strategy.

**Technology solutions**

Security equipment and visual monitoring equipment are not a panacea and must be used as one tool in the task of providing security for the hospital. That said, equipment can be very effective to provide early warning of potential threats and give the security team time to respond...
effectively, especially when they are integrated into a common backbone. Here are some examples of today's technologies:

- **Access controls.** Proximity or smart cards and biometric sensors (voice, hand readers, facial recognition, and fingerprint-ridge pattern analysis) can secure doors and barriers from entry by unauthorized persons into areas that require high levels of security. These may include drug-dispensing storage and pharmacy rooms, which are common areas of interest for addicts and criminals intent on stealing drugs for street sale. Additionally, areas where newborns are kept have been targeted in incidents in which infants have been carried off by people posing as hospital staff. Controlled access through doors in these areas can help stop these types of crimes.

- **Identification.** Wrist and ankle bracelets equipped with Radio Frequency Identification (RFID) tags can track wandering patients who may have dementia, or babies who might be subject to kidnapping. Using these tags, hospitals can lock doors as patients approach exits, generate alarms and alert nursing and safety staff of the attempted breach of security. RFID can also be used for equipment tracking and asset management.

- **Parking and site entry security.** Hospitals provide controlled access into and out of parking areas using a variety of electronic sensors on staff and hospital-owned vehicles. These devices can keep vehicles from being removed from secured areas, and protect staff as they walk to and from their vehicles.

  The devices can also be combined with other solutions for homeland security applications. Using access control, installing bollard systems and physical barriers and enforcing minimum standoff distances can protect structures from catastrophic collapse resulting from vehicle-borne explosive devices, if a risk assessment calls for such measures.

  Hospitals should also strongly consider locating emergency telephones at strategic points in the parking garage or area.

- **Camera technology.** Cameras allow security teams to have "eyes" in many places on campus without having a physical presence. There are basic cameras available as well as digital video recording devices and more complex devices.

  For instance, facial recognition cameras recognize specific facial/bone structures and the overlying musculature features to provide access control for staff and patients. These cameras and embedded processors cannot be fooled by lifelike masks, as they look for micro-movement of facial muscles in order to validate an entry request. They are hands-free and can be maintained in sterile environments, thus allowing staff to avoid contact with contaminated surfaces.

  Likewise, day/night cameras are daytime high-resolution color cameras that have 20 times zoom lenses for viewing visitors, vehicles and their license plates, and then autoswitching to monochrome mode under low-light conditions. These cameras can autonomously track movement within their field of view, return to a “home” position when no movement is detected, and wait for the next activity by humans or vehicles.

  A thermal cameras is another type of device that sees infrared emissions from all living and inanimate objects. Neither
sunlight nor artificial lighting is needed for adequate viewing ability. These cameras give security staff a phenomenally enhanced vision boost to identify areas outside the hospital where criminals may lurk. In areas where lighting will not penetrate or aesthetics and good neighbor relations demand a lowered visible lighting level, thermal imaging fills the need for nighttime viewing by the security staff. Privacy is also maintained as thermal cameras cannot view through glass.

- **Motion sensing systems.** There are many outdoor motion sensing systems. The newest and least expensive of the dependable ones is a specialized video-based motion detection processor that excludes virtually all nonhuman-based forms of motion. Pixel-change motion detection systems have been available for two decades, but recent advancements in high-speed computerized processing and adaptive algorithms now allow systems to sample existing or new video feeds to determine if a human form is attempting to enter or leave any area under surveillance. Lighting changes and spurious movement from small animals, birds or insects are automatically filtered out and excluded from alert because the system has over 100,000 images of human forms and can extrapolate what a human can and cannot do. Using these systems in an autonomous fashion, the centralized proprietary guards can focus their energies and time to monitor areas of high-activity or concern while relying on enhanced electronics to alert them of danger and intrusion activity.

- **IT access control.** In addition to the above-mentioned physical security technologies are any number of data security systems to protect patient health and personal records in accordance with the Health Insurance Portability and Accountability Act (HIPPA).

**Systems integration**

Full systems integration makes it possible to link sensors and devices into seamless automated command sequences. Consequently, hand-in-hand with security equipment planning is the need to build infrastructure to support the technology installation. System designs and equipment installation can be scaled and implemented in a measured way over time and as budgets allow, but a robust wiring infrastructure should be planned for and installed up front, if possible.

Under an integrated system, a panic alarm activation in the pharmacy, for instance, can result in lights being activated, doors opened or closed, and pre-recorded voices warning staff in the vicinity to avoid certain areas where they might encounter an armed suspect. Camera images of the suspect and staff can immediately be transmitted to the responding police agency and officers in their patrol cars, a holdup alarm can be transmitted to the police dispatch via high-priority e-mail, hospital security staff can view the images in live mode from small handheld portable monitors, and cameras can track the suspect from anywhere within the hospital to their vehicle within visual range of the hospital. "Convergence" is often used to describe how various technologies (such as voice and data) that were once separate are now becoming one system through common cabling. This term can be applied to security technology as well.

Many (if not all) camera and access control technologies can ride on the hospital's Ethernet system and are driven by server-based head ends. It is recommended that hospitals consider an application-independent cabling system (sometimes referred to as "structured cabling"). This system essentially builds an information superhighway that allows technologies to be added at any time, similar to on- and off-ramps on the highway. The advantage is
that one can plan for the ultimate security installation and get the cabling infrastructure at a relatively lower cost than adding it at a later date.

**The human element**

Technology should serve to complement the security's human element. This involves roving security guards that monitor remote locations and show a presence on campus.

Monitoring equipment can be used to supplement the security team's eyes, but guards can act as prevention or help someone in need. Having guards roam in tandem with monitoring equipment and good communications enhances the level of security and safety within the campus environment.

A comprehensive set of policies that govern how security is administered, training procedures and how to quickly respond to security instances goes a long way toward creating a safe environment and can help reduce the need for some expensive equipment.

Capitalizing on the vast numbers of clinical and administrative staff, hospitals can train employees to be aware of security issues around them, providing a level of security that is ubiquitous in all areas of the facility. Like security guards, hospital clinical and administrative staff can provide monitoring, prevention and intervention duties at the same time.

**Bottom line**

The electronic tools available to the security, facilities and risk managers who are responsible for keeping hospitals safe can be truly life saving.

Employing them requires a reasoned and balanced approach that directs available finances to the most pressing needs and balances them with simple no-cost policy and procedural changes that bolster human security.

The bottom line is to invest up front in good risk assessment, systems planning and infrastructure, then implement the plan in a measured way that coincides with available budget and phases of construction.

*Tom Leonidas, Jr., P.E. is managing partner at Sparling, a Seattle-based electrical and technology consulting firm that specializes in health care planning and design. He can be reached at tleonidas@sparling.com  Jim O'Donnell is president and owner of Statewide Security, Redmond, Wash., and is a former law enforcement officer with 27 years in the high-tech security industry. He can be reached at swidejimodonnell@aol.com.*