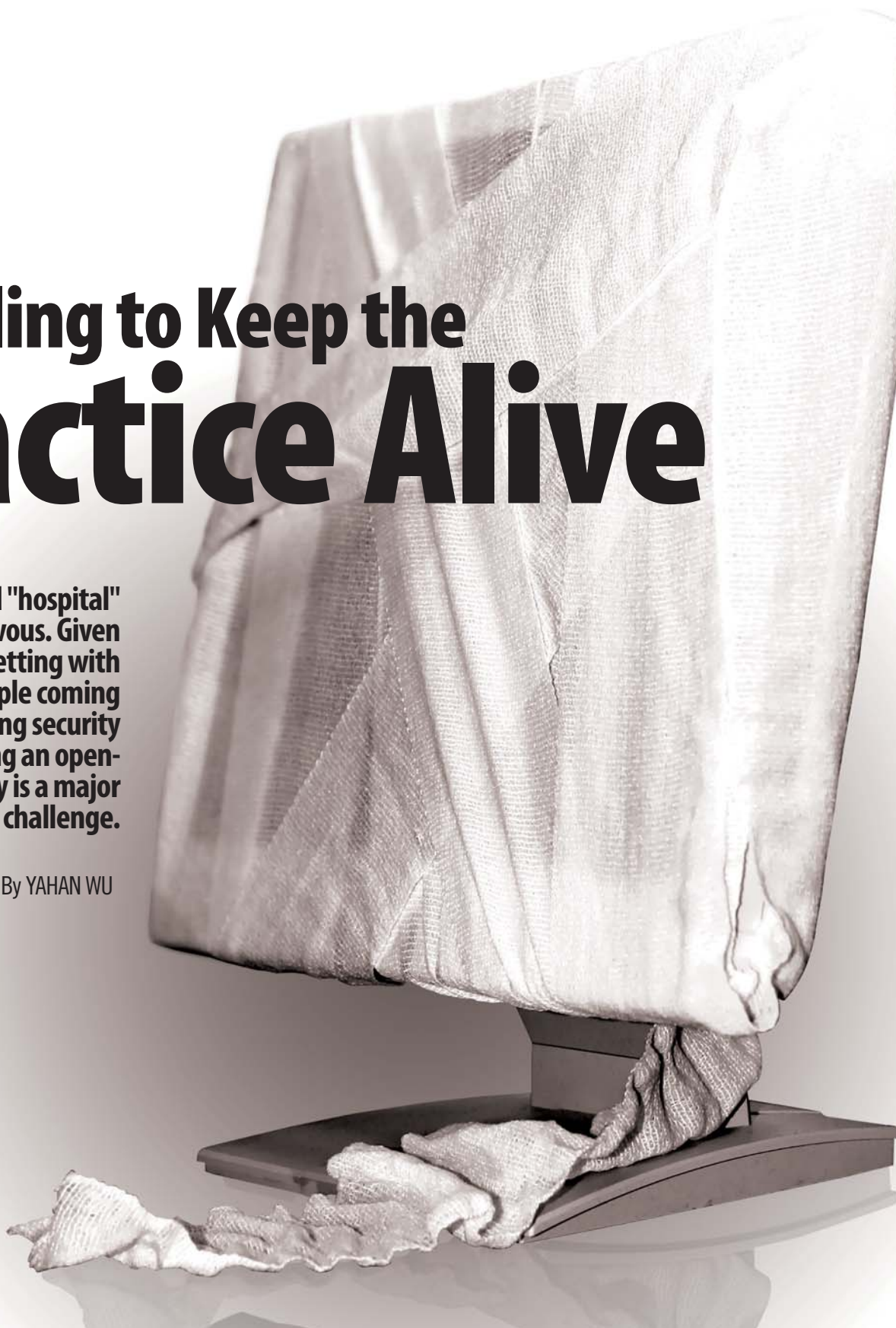
Struggling to Keep the Practice Alive

Even the word "hospital" makes people nervous. Given the high-paced setting with all kinds of people coming and going, providing security while preserving an open-door policy is a major challenge.

By YAHAN WU



"Hospitals and churches have always been considered sacred, at least as far back as I can remember," said Jeff Aldridge, president of Security Assessments International (SAI), a U.S.-based consulting firm specializing in hospital security. For the past 18 years, SAI has helped hospitals identify and control loss and reduce risks through security-assessment programs.

He said a few decades ago, it was unimaginable that anyone would violate the sanctity of a hospital by, for example, kidnapping a baby. Hospitals are institutions of tradition, and historically have resisted becoming well-fortified. Rather, the focus has always been on giving open, friendly access to the public despite such threats.

Violence Primary Market Driver

"I would say the primary driver for security installations in hospitals is increased violence," said Dominic Bruning, EMEA marketing director for Axis Communications. While the main threat, he explained, is against staff, other patients could also be attacked. Hospitals have a responsibility to both.

The following statistics paint a chilling picture of the risks hospital staff and patients face. According to a report by the Guardian in April 2001, violence in hospitals had become so widespread that, on average, 500 violent incidents took place at every National Health Service (NHS) Trust in the U.K. in 2000. In almost all major teaching hospitals, police presence is now routine, especially around hotspots like Accident and Emergency (A&E) departments.

NHS trusts are also employing their own security guards, hiring private companies to carry out round-the-clock patrols, using surveillance and alarms, and, in some cases, giving staff mobile phones and pagers. Staff accommodation has to be protected from intruders as well and trusts have introduced tight security in maternity units because of baby snatching. Finally, many hospitals are plagued by thieves and vandals.

Phillip Launt, director of business development at SAI

It is the same in the U.S. Phillip Launt, director of business development at SAI, said healthcare security is now among the fastest-growing market segments. "It is safe to say healthcare security is a multibillion-dollar business; growth is projected for the next five to eight years."

One reason is that hospitals are still years behind the security curve. Another factor, as mentioned, is that violence in the healthcare setting has increased dramatically; this has focused attention on security's counterpart: liability. Launt believes that following the Sept. 11 terrorist attacks, hospitals must prepare for mass casualties. In addition, hospitals, themselves, are now potential targets.

A 2005 survey by SAI on emergency-department nurses in Pennsylvania showed that 97 percent reported verbal abuse, 94 percent had received physical threats, 66 percent were physically assaulted, 25 percent of all nurse assaults occurred in the emergency department (ED), and of the 51 nurse homicides reported, 23 percent occurred in the ED. A recent Emergency Nurses Association study revealed that 82 percent of nurses surveyed had been assaulted some time during their careers, yet a significant number of assaults were not reported.

Poles Apart

Security installations in hospitals are very diffierent from those used in other applications. "If a hospital were to be viewed as just another facility to secure, then the approach to installing security equipment, such as mechanical locks, electronic access-control devices, CCTVs, RFID-tagging systems, panic alarms, security lighting, would differ little from other installations," said Launt.

"To view a hospital in this light would be extremely short-sighted because the hospital environment is unique. Hospitals are, in reality, cities unto themselves. They operate 24 hours a day, seven days a week, facing all the security issues that a small city or thriving community faces. Going one step further, every hospital has its own security threats, vulnerabilities and security requirements."

Environment of care standards and best practices in the U.S. require that hospitals provide a reasonable level of security for patients, visitors and employees. Hospitals are also looking at ways to protect high-value medical equipment used in direct patient care. These security requirements, standards and mandates are addressed through security-management plans.

Installation of common security components during new hospital construction is closest to retail and government sectors. However, hospitals require different types of security equipment and systems not common in other markets. Installation of mechanical door locks with master-key systems, for example, is fairly well standardized across all vertical markets, while infant-protection, mother-baby mixup-prevention, wandering-patient, nurse-call and pharmaceutical-dispensing systems are unique.

Bruning pinpointed lack of physical space to run additional cabling. This makes wireless surveillance and deployments utilizing existing Cat 5e network infrastructure appealing. Other security pressures arise in patient-waiting areas, such as in A&E where patients, themselves, can be security risks to other waiting patients or staff, such as porters, nurses and receptionists. Numerous hospitals have existing analog CCTV systems, which can be upgraded to provide easier access to other key members of staff by distributing video across networks.

Frequently, at hospitals, security directors are continually at odds with administration over types of security involved as well as visibility levels. "Administrators of healthcare facilities, perhaps more than any other type of institution, are tuned into public perceptions. In this regard, they seek to convey a sense of safety and security to patients, visitors and staff," Launt elaborated. Which methods are often subject to debate. "Long, heated discussions are known to have taken place over what type of security equipment to use, how visible to make it, what access-control measures to implement and a myriad of other issues."

"The security department will inevitably favor maximum visibility and exposure, such as uniformed security guards, highly visible CCTVs, access-control devices, metal detectors and security placards. Administrations typically lean toward more discreet, less obtrusive security measures so as not to raise patient fears or anxiety. A security consultant can often point the way to a compromise between extremes that will ensure adequate security for the hospital without giving it the appearance of an armed encampment."

Metal detectors, for example, can be designed and deployed in such a way as to make them virtually invisible. CCTV technology also makes it possible to locate and position cameras for maximum-security coverage without being obtrusive. When these measures are combined with appropriate security placards, the public is informed about measures in place without causing unnecessary anxiety. Another point is that security and convenience are at opposite ends of the scale. As security increases, convenience decreases; as system convenience goes up, security goes down. Please refer to the box for a list of priority areas in hospital security.

Hospital Priority Areas

1. Cashier: Any room where cash is counted and stored should be locked at all times with extremely tight controls on operating keys.
2. Administration/Human Resources: All personnel and patient files are stored here. Computers and other office equipment are also prevalent. Only management and security personnel should have keys to these areas.
3. Pharmacy: Doctors and nurses increasingly abuse drugs. Strict key control of pharmacies is essential. Also, all carts and cabinets containing pharmaceuticals outside pharmacies need to be on the same key system.
4. Psychiatric Unit: Extremely sensitive patient records, often pertaining to criminal cases, as well as prescription drugs are kept here. Keys should be restricted to department and security personnel.
5. Nursery: One of the worst fears of any hospital is kidnapping of newborns. While extremely rare, resulting publicity and liability is an absolute nightmare.
6. Tool Crib: Often overlooked, this area contains many items which can be stolen and resold easily. If padlocks are required, they should have the capabilities of being keyed into existing master-key systems. No personnel outside maintenance and security should possess operating keys.

Sean Shankar, vice president of marketing at IntelliVision

Installation Snags

A safe hospital means everyone has to be identified and their access controlled. Aldridge pointed out some difficulties healthcare facilities have faced in the past. Access control has been extremely difficult before because of unrealistic and misinterpreted fire codes. Strict enforcement of fire codes has prevented hospitals from securing fire doors that lead to the outside. An unsecured fire door leading to the outside provides an escape route for criminals.

"After what seems like forever," he said, "old fire codes are now being replaced with new codes that allow fire exits to be locked and alarmed by a time-delay lock and alarm system. This type of lockdown capability can prevent unauthorized persons from entering or leaving the hospital undetected."

Another significant problem with providing security for older hospitals is their inherently open design. Traditionally, hospitals have been designed for patient and family convenience. Security, said Aldridge, was never taken into consideration during design and construction. "Because of this, retrofitting security protection in older facilities is a security nightmare, not to mention unbelievably expensive."

Another problem is radio frequency. According to Launt, healthcare environments are RF-rich and getting richer with the advent of new medical equipment, Wi-Fi and RFID systems. RF systems installed in hospitals must be installed, aligned and calibrated with great care so that they operate properly yet do not interfere with other patient-care equipment. This is, perhaps, the greatest challenge to system integrators and installers.

Last, the bottom line is patient care. All security systems must function in harmony with work practices and procedures employed by nurses, doctors and other staff as they go about their primary mission: taking care of patients.

Moving Uptown

"I believe that the majority of hospitals still have existing or rapidly aging analog CCTV systems that are in need of

upgrading and replacing," said Bruning. "Most systems will have limited or no integration with other security systems." As in other markets, this is starting to change. Hospitals are finding total solutions for security needs as well as integration. The latter, he continued, is driving growth as disparate systems can be brought together to provide improvements in productivity and real-time actionable data.

In terms of equipment and systems, the trend is toward all-digital color camera and archiving systems, multipurpose integrated access-control systems, and biometrics for sensitive areas, Launt reported. "Recently, we have also noted a trend toward employing contract guard services to replace or augment the more traditional inhouse security force. In our opinion, this is not a positive development."

Paralleling these developments are two other major happenings: first is convergence of physical and IT (logical) security; second is large security-integration companies, which have embraced the concept of providing total security solutions.

Hospital administrators now have options beyond the old piecemeal application of band-aid patches to outdated systems. Under the new paradigm, administrators work closely with security consultants and integrators to design, budget, implement and maintain total security solutions that meet their current requirements and future needs.

Sean Shankar, vice president of marketing at IntelliVision, said hospitals in the U.S. are just beginning to use intelligent video for patient monitoring. He estimated company revenues to be three percent or less of sales volume in the market. Typically, this is for monitoring inpatients as hospital staff are spread too thin to ensure patients are doing fine, especially at night. The technology is also used to assist in detecting and alerting hospital staff to patient movements.

Courtesy of SAI

Landing the Contract

Hospital contracts are comparable to those of college campuses or office parks. Both scenarios involve responding to request for proposals (RFP); both require consultation with prospective clients to determine scope of work. "We know from experience," said Launt, "that hospital projects are apt to involve review by one or more committees. There is seldom one decision-maker calling the shots. Budgetary issues are also paramount."

Contracts are usually awarded based on proposal strength, project cost, company reputation, consultant capability and ability to deliver services defined. The main contact is usually the security director. Seminars are another source of potential installers and equipment vendors. One example is the International Association for Healthcare Security and Safety (IAHSS), which holds an annual seminar where exhibitors can display security products and services.

Yet another is hospital renovations. It is important to identify construction projects early on. One way to get a leg-up, at least in the U.S., is by keeping up with construction projects granted by the federal Health Resources and Services Administration (HRSA), a division of the U.S. Department of Health and Human Services. The HRSA provides resources to expand health-care facilities across the country. An easy way to find which medical facilities are receiving HRSA grants is to click on the grants area of the HRSA's Web site at www.hrsa.gov/grants. There are additional government and private bid opportunities available on the LeadTracker Web site at www.ssileadtracker.com.

Although hospitals generally rely on bigger brands for standard products, there is hope for the little guys. Bruning said, in his experience, smaller, niche companies with good track records have a chance. "I believe that, like most end-user organizations, the solution delivered is more important than the brand of the individual components. This may have been the case in traditional analog installations, but moving forward, I believe that integrators and consultants will play a more important role in specifying the total solution." He also pointed out that as systems become more advanced with, say, intelligent applications integrated with biometric readers, factors other than pure branding come into their own. AS