It Will Never Happen Here, Right?

Most healthcare organizations and physician office practices consider security a low priority item. Many hospitals, nursing facilities, diagnostic imaging centers, assisted living centers, and freestanding ambulatory surgery centers share this attitude. Such attitudes are not shared by all in the healthcare community, especially those with buildings and parking garages located in well-known, high-crime areas.

Armed and unarmed security personnel patrol the perimeter of such locations and many buildings and garages are monitored via surveillance camera for potential security risks. Where risks are high, some healthcare organizations have embarked upon a visible presence of security even within key areas of a building.

For many years there was a sense that we are “okay” in rural and suburban healthcare settings. Many in small towns and cities shared that same sense of security across the land. Hence, security resources were not a top priority. When challenged the response was, “Do not worry. It will never happen here.”

Times have changed. Post 9/11 incidents and discussions of bioterrorism have led some to realize the vulnerability of any healthcare facility as the site of a terrorist attack; healthcare facilities are the proverbial “soft target.”

The increase in gang violence spilling into suburbs has seen gun-wielding assailants pursue injured victims into emergency departments. Drug-seeking behavior has resulted in attacks on freestanding facilities and physician office practices. Still others have seen disturbing behavior, such as unknown individuals drive up to a healthcare facility, snap video or photographs and then drive away. A trace of license plates reveals that often the car or vehicle is stolen, or that it was rented by someone whose identity cannot be verified.
Is it right to continue to say, “It will not happen here!” Is this a statement of fact, or a false hope? As suggested here, the problem is one that is far broader, involving risks not only from outside a healthcare organization, but also from within the confines of a hospital, nursing home or another type of facility.

**Security Risk Examples.**

Security risks can happen in any healthcare organization and at any time. The risk may involve an external source, an intrusion. The risk may come from within the healthcare organization at the hands of a disgruntled staff member. The targets of security risks may be patients, staff members, or the facility’ assets— including equipment or records. Some examples illustrate the scope of the problem:

*The Risk of the Dental Office Intruder* – A California man involved in what was described as a domestic dispute entered a dental office shooting five people. The one person who died in the assault was believed to have been the wife of the shooter.¹

*When a Co-Worker is the Shooter* – A hospital pharmacy worker entered the healthcare facility and shot and killed two of his managers before taking his own life. People who knew the assailant described him as a person who was, “smiling, laughing, making sure everybody was doing OK.”²

*Why Long Term Care is Not Immune* – On a Sunday morning, a man entered a rural, North Carolina nursing home and opened fire, killing seven elderly residents and a nurse. A police officer who confronted the assailant was also shot. Two others also were injured in the attack.³

*When the Weapon of Choice is Not a Gun* – On a Saturday morning the estranged boyfriend of a recovery room nurse entered a Windsor, Ontario hospital armed with a knife. The boyfriend was an anesthesiologist on staff at the hospital. The nurse had told hospital leadership that she feared that he would harm her. The hospital assisted her in getting a lawyer who planned to secure a temporary restraining order on the following Tuesday. The nurse was placed on a different shift and she was provided with an escort to the parking garage. This proved futile when the physician stabbed her to death inside the hospital. He then withdrew controlled drugs and syringes from a locked cabinet, drove over to a spot overlooking the Detroit River and injected himself with a lethal combination.⁴
**When the Security Risk Involves a Sexual Assault** – a young nurse's assistant at a nursing home in Texas was discovered by a fellow employee to be sexually assaulting an eighty-two year old resident who suffered from Alzheimer's disease. The nursing assistant was found guilty of aggravated sexual assault and sentenced to 15 years in prison.⁵

**When the Security Risk is a Family Member** – A man was admitted to a North Carolina hospital suffering from severe heart disease, hypertension, a thoracic aneurysm, and several pulmonary emboli. It was determined that his condition was untreatable and terminal. A “No Code,” order was issued for the patient. When the patient’s adult son came to see him he shot the patient in the head four times at point blank range. The assailant told police, “You can't do anything to him now. He's out of his suffering.” “I killed my daddy.” “He won't have to suffer anymore.” “I know they can burn me for it, but my dad will not have to suffer anymore.” “I know the doctors couldn't do it, but I could.” “I promised my dad I wouldn't let him suffer.”⁶

**The Choice of “Weapons” May Prove Alarming.**
Security risks need not involve handguns, rifles, or knives. Sometimes equipment found in a healthcare organization can be transformed into a weapon of choice. A scalpel hurled by a disruptive care provider in the operating room strikes and penetrates the arm of a nurse just entering the room. The valves for flammable or noxious gasses intentionally turned on. A patient awaiting treatment in the emergency department grabs an IV pole, swinging it hard against the head of an emergency room technician; the employee sustains a skull fracture.

Sometimes the security risk can be more insidious. A person who wants to obtain narcotics from the outpatient pharmacy releases pepper spray or another noxious substance into the intake air duct or pulls the nearby fire alarm. Staff exit and the perpetrator enters in the confusion.

With increasing reliance on computerized systems for a variety of healthcare facility operations, a serious security risk involves computer criminals (“crackers”) who take control of vital systems. Such was the allegation raised in a recent situation in Texas in which an overnight security officer gained control of a healthcare facility’s HVAC system.⁷ Such a risk goes well beyond identity theft and data breaches; it goes to the core of maintaining a safe and secure environment of care. If HVAC systems can be penetrated in this way, what could happen to security doors, smart pumps, implantable devices, water and gas systems, and other programmable devices? This is particularly worrisome if the
devices, or the networks they are connected to have wireless capability, giving an attacker the ability to possibly penetrate the systems from well beyond the facility’s perimeter using a high-gain or amplified antenna.

The Fall of 2009 may introduce yet another, powerful security risk for healthcare organizations that does not involve the use of weapons: a surge of patients seeking treatment for H1N1 Novel A Influenza. An epidemic carries with it more than the risk of serious illness or death. Employees may become patients themselves, leaving healthcare facilities ill-equipped to handle an onslaught of people suffering from H1N1 Novel A. Those employees afflicted with the illness may be part of the security contingent. Others must be poised to fill the gap and work collaboratively with colleagues from other healthcare organizations and emergency management authorities. The point is, however, that a pandemic has the potential to become a potent security risk for healthcare organizations.

**Why It Can Happen Here – Now.**
Recent reports demonstrate reason for concern about security risks in healthcare settings. According to data compiled by Anthony N. Potter, a well-respected health care security specialist based in North Carolina, from 2008 through July 2009, 39 people have died in hospital incidents that included a firearm or officer fatalities. In a survey published in the *Journal of Nursing Administration* involving emergency nursing professionals, more than half reported having been the subject of physical assaults in the workplace.

What is causing such security problems? Is it as one police official suggested a reflection of the tension in today’s society, or are there other plausible reasons? No doubt, the healthcare field has felt the impact of the lingering recession. Patients who have stopped taking medication to control behavioral issues may end up receiving emergent care in the emergency departments of acute care facilities. Such patients can become disruptive and combative in the healthcare setting. The loss of employment and the inability to pay for COBRA coverage may fan the flames of despair and anger, leading to some acting out their frustrations in a hospital or a physician practice.

Healthcare facilities have been compelled to make difficult choices, curtailing the number of staff, consolidating operations such as safety and security, and reducing the number of personnel available to handle security matters.

Although many have come to recognize the issue of disruptive behavior in the healthcare field, there is much room for improvement in exerting leadership to
address troubled care providers. Instead of confronting the problem directly, enabling unacceptable conduct continues in some healthcare organizations. The result may be a contributing cause for concern in healthcare security.

The financial cost may also be a problem. Security is not a revenue-generator in the healthcare field. However, the absence of it can prove costly, particularly if an event occurs that results in infant or child abduction, a sexual assault of a patient, or the death of an employee at the hands of a disturbed individual in the emergency department. Violence that results in severe back or hand injuries to an employee can help drive up the costs of workers’ compensation coverage. Those who have been the victims of physical assaults or witness such actions in the healthcare setting may decide to seek employment in less risk prone settings. Staff recruitment and training costs, litigation costs and workers’ compensation claims can be expensive. The cost of reputational loss in the community following a serious event may also be extremely damaging. Of concern too, is that new personnel may lack the skill set or critical thinking required to handle emerging security issues. It is for these reasons it may imprudent to say, “It will never happen here, right?”

Like risk management, healthcare security is a specific discipline. It requires specialized training and development of organizational security programs that are consistent with recognized guidelines such as the IAHSS Healthcare Security: Industry Guidelines, 2009.12

The fact that someone has completed a degree in criminal justice or works as a police officer in a local police department does not suggest he or she is qualified to work as a security professional in a healthcare setting. Courses and certification programs are available from IAHSS.13 But even with this level of education, situational awareness is important. To be successful, healthcare security professionals, like their risk management colleagues, have to understand the culture of the organization and the environment and the local community.

Risk management interacts with others in the security world. Those responsible for IT security are important players in creating an effective environment of care. The same is true for local police, fire, and emergency management organizations. The lack of awareness and communication with such constituencies can create unnecessary risk exposure.
Whether it is relationships within a healthcare organization or with outside agencies, risk management professionals would do well to take the initiative and develop lines of communication. Taking such an approach can prove crucial in the course of serious security situations.

**Risk Management Strategies for Healthcare Security.**

Healthcare organization security is an area ripe for enterprise risk management. The ability to operate and maintain a secure environment of care impacts all aspects of a healthcare organization or physician practice. Utilizing solid principles found in enterprise risk management, much could be done to identify and address security vulnerabilities in a healthcare organization. This includes the following strategies.

1. **Complete an Internal Security Assessment.**
   Work with security professionals in the healthcare organization to assess security strengths and weaknesses. Recognize that the assessment should be organization-specific, so that if the organization operates a large unit for inpatient substance abuse treatment or a long term care facility for dementia residents, the evaluation should be adapted to address the specific risks for such vulnerable areas.

2. **Analyze External Security Risks.**
   Use reliable data from local, state, and national sources to evaluate external security threats to the healthcare organization. Understand that such an approach should be done on a regular basis, taking into consideration changes in demographics, gang activity, and emerging IT threats that may have a negative impact on vulnerable computer and medical device systems.

3. **Complete a SWOT Evaluation.**
   Use the data from both the internal and external assessments to complete an enterprise-wide Strengths-Weaknesses-Opportunities-Threat or SWOT evaluation of security risks. Consider too, using an Opportunity Analysis-style Failure Mode and Effect Analysis (FMEA) to set priorities for short-term and long-term action steps.

4. **Emphasize the ROI of Effective Security.**
   Calculate the return on investment (ROI) of implementing recommended improvements derived from the SWOT evaluation. Provide leadership with concrete short-term and long-term ROI data.
and contrast this information with projected costs of maintaining the status quo. For example, consider for this latter purpose actual and projected workers’ compensation claims data and coverages cost.

5. **Provide Enterprise Risk Management Recommendations.**
Utilize the SWOT evaluation to profile ERM style recommendations for the healthcare organization. Looking beyond liability claim costs for such risks as infant and child abduction or workers’ compensation claims and coverage. Consider too, the cost of risks stemming from investigations of alleged assaults, IT breaches, regulatory compliance reviews and responses, staff turnover, and reputational loss. Use this data to project what the financial impact may be to the healthcare organization. Make practical enterprise-wide recommendations for security throughout the healthcare organization.

6. **Institute Enterprise-Wide Security Education.**
Work with colleagues in security to incorporate throughout the healthcare organization practically oriented education from orientation through regular in-service programs. Emphasize the importance of situational awareness, critical thinking, and timely communication. Demonstrate how “chain of command” can be used to address security issues.

7. **Stress Test Redundant Communication Systems.**
Collaborate with colleagues in telecommunications, IT and security services to test communication systems for back-up during outages, IT breaches, and disaster situations. Implement needed improvements for identified vulnerabilities with both internal and external security communication systems.

8. **Make Security an Enterprise Team Member.**
Do not limit the role of security services in an enterprise risk management system. Encourage active participation with other key stakeholders in the organization, including human resources, patient safety, and healthcare facility renovation and new construction. Recognize that the skill sets found among security service professionals can help with sensitive internal investigations as well as complicated criminal background checks for would-be new hires.
**Conclusion.**

From the spillover effects of domestic violence to potential terrorist threats to the potential for an onslaught of patients suffering from H1N1 Novel Influenza A, security risks present a serious challenge to healthcare organizations and physician practices. Recent events have shown that no area of the country is “safe” from serious security exposures in the healthcare industry. As such, complacent attitudes are not acceptable. No one should feel confident to say, “It will never happen here, right?”

A more realistic, balanced approach is needed. Those who work in healthcare facilities vulnerable for gang activity or that have high-risk patient populations need no reminder of the importance of taking prudent steps to enhance security.

Those who perceive themselves to be “okay” may be deluding themselves and doing a disservice to the community. Infant and child abduction can occur in any acute care facility. A drug-crazed person can enter any physician practice brandishing gun while demanding narcotics. An irate husband who has lost his job and had a nasty spate with his spouse may decide to take his anger out on a group of innocent, elderly dementia patients in the facility in which his wife serves as a nursing assistant. Such events can happen at anytime and anywhere in the country.

Using a practical enterprise risk management approach, organizations can take steps now to address the potential for such unsettling occurrences. Such an approach requires careful analysis, priority-setting, education, and good communication. Such an approach also requires respect for and active involvement of healthcare security professionals who can help make a difference in creating a safe and secure environment in the healthcare arena.

*If you would like assistance with developing an enterprise risk management program, please contact us at (860) 242-1302.*
1 “One Dead 4 Hurt in California Rampage,” AP as reported at www.msnbc.com, July 2, 2009.


8 As the World Health Organization has noted:
   “Even if the current pattern of usually mild illness continues, the impact of the pandemic during the second wave could worsen as larger numbers of people become infected. Larger numbers of severely ill patients requiring intensive care are likely to be the most urgent burden on health services, creating pressures that could overwhelm intensive care units and possibly disrupt the provision of care for other diseases.”

9 See, A. N. Potter, “Hospital Incidents Involving Firearms or Officer Deaths in 2008-2009 to Date.” Part of the data for this analysis was taken from IAHSS Healthcare Safety & Security Directions, Vol. 22, No. 1 (2009). The rest was collected from various news sources.


11 Co-Workers Describe Shooter as a Joking Family Man,” by A. Taxin, Associated Press, April 17, 2009.

12 The International Association for Healthcare Security and Safety or IAHSS guidelines can be found at http://www.iahss.org/About/Guidelines.asp.

13 See, www.iahss.org for information on educational and certification programs.