

# The Workplace Violence Epidemic

*In the high-tension  
hospital atmosphere,  
threats must be mitigated  
by diligent adaptation of  
security policies and  
procedures*

**T**he challenges of securing employees, assets, clients and facilities can be difficult to meet in any environment; however, few organizations must contend with the level of daily turbulence and pressure that hospitals do. Changes due to federal health reform, compliance with data protection laws and employee safety directives, shifts in demographics and service philosophy, and increasing crime must all be addressed without inhibiting public access, reducing the speed of service, or enhancing patient discomfort and stress.

The practice of security in hospitals has rapidly evolved over the past five years and continues to adapt to new challenges as it improves its response.

## **Increasing Workplace Violence Attracting Attention**

The idea of a formal security program is fairly new in many hospitals, says David Gibbs, a managing director at Guidepost Solutions, a low-voltage consulting and design firm with 30 years of experience in the healthcare market. Gibbs is a regional chairperson for the International Association for Healthcare Security and Safety (IAHSS) and is heavily involved in ASHE, the American Society for Healthcare Engineering.

Traditionally, hospital facilities directors and building engineers have taken on security and safety responsibilities, says Gibbs, but many hospitals he's worked with — particularly smaller or more rural facilities — had no security to speak of. "That's all dramatically changed in the last five years as the overall frequency of physical violence and verbal abuse has spiked. This has had a dramatic impact at the C level," Gibbs says.

A 2010 survey by IAHSS reported that in four categories — sexual assault, robbery, aggravated assault, and simple assault — violent crime in hospitals increased by 200 percent from 2004-2009. Other studies bear out similar findings. The Joint Commission's Sentinel Event Database, which tracks unexpected events resulting in death or serious injury, shows that 2011 had the second-highest reported rate of criminal events since the database's inception in 1995, and that data only covered events reported through the third quarter of the year. The Emergency Department Violence Surveillance Study released by the

Emergency Nurses Association in Nov. 2011 found that of more than 6,500 emergency department nurses surveyed, 54.5 percent had experienced physical violence and/or verbal abuse at work at some point in the previous seven days.

“The high-tension atmosphere of a hospital is unequalled in any other industry,” says Bonnie Michelman, Director of Police, Security and Outside Services at Massachusetts General Hospital, a member of the Security Executive Council. “People are at their worst, in fear and pain. People equate being in a hospital with a loss of freedom and dignity. Visitors are upset, and there are a lot of vulnerable people who are not ambulatory or mentally competent or rational,” she says.

These tensions have always been a part of the hospital risk landscape, but Michelman and others are seeing more drug addicted, suicidal and mentally unstable patients coming into the emergency department. In effect, this combines the most high-pressure, busiest and most publicly accessible area in the hospital with some of the most unpredictable, potentially violent patients. The IAHS further reports that increased gang activity and increased unemployment play a role in the crime spike.

In the face of the dramatic increase in violence — most of which is violence against nurses by patients in emergency and psychiatric departments — hospitals are seeing an increase in healthcare-specific regulatory oversight of workplace violence, according to Bryan Warren, Senior Manager of Corporate Security at Carolinas Healthcare System and president of IAHS. Guidance and recommendations for workplace violence prevention in hospitals have existed for years in the form of OSHA 3148, whose latest version was released in 2004; but, OSHA published a new directive in Sept. 2011 specifically targeting healthcare as one of several high-risk environments that warrant special attention. “The new directive addresses the need for much more workplace violence prevention training, using specific healthcare examples,” Warren says.

“Workplace violence is part of an epidemic in healthcare now, and line staff



**“The high-tension atmosphere of a hospital is unequalled in any other industry,” says Bonnie Michelman of Massachusetts General Hospital.**

— regardless of what unit they work in — must have at least a basic knowledge of how to recognize potential warning signs and how to react appropriately when an incident occurs,” he continues. “That’s the bare minimum, regardless of facility size, location or hours of operation. Only then can we start looking at the security staffing or engineering controls to help prevent these incidents. Workplace violence isn’t something you can solve by putting in a lock and a camera. You have to have the human component with the ability to recognize and report so the proper mitigation can be undertaken.”

Michelman agrees that training is the key, and that it must be done right. “Doing fun, dynamic training that people enjoy is the most effective

approach. We offer many different training programs, and our goal is to make them enjoyable exercises rather than tedious meetings,” she says.

Reporting policies — especially zero-tolerance policies — are a main factor of decreased violence potential noted in the Emergency Nurses Association study, along with management commitment to workplace violence control. The use of a panic button and enclosed nurses’ stations, locked/coded emergency department entry, security signage and well-lit areas were also associated with lower levels of physical and verbal violence.

An excellent security staff is a critical element in the reduction of workplace violence incidents as well, Michelman adds. “You need well-

**economical mantrap controller**

*Ashley,  
How this economical  
controller has  
intelligent control  
and an LED timer!  
Richard*

Dortronics new economical 4700 series Mantrap Controllers have factory pre-programmed PLC intelligent control with optional timer logic and LED display. It's factory programmed to allow only one door, in any defined area, to be unsecured at a time. Simultaneous requests for access or requests for access while another door is unsecured are denied to maintain the highest level of control. It's also compatible with any access control system. Packaged complete with 12/24 VDC power supply for maglocks and/or strikes.

**DORTRONICS SYSTEMS, INC.**

dortronics.com • sales@dortronics.com • 1-800-906-0137

## Metrics in Healthcare Security

The financial picture for hospitals over the next 10 years is muddy. Many reports project that hospitals — particularly large or urban hospitals — will gain patients and revenue from the increase in insured Americans as a result of healthcare reform. However, changes in Medicare and Medicaid reimbursements will take a toll on those revenues. One thing is clear: hospitals are moving forward with caution.

“I think with the state of healthcare reimbursement and reform, every hospital has had to tighten its belt and will continue to have to do so,” says Bonnie Michelman, Director of Police, Security and Outside Services at Massachusetts General Hospital. Michelman is one of the founding members of a working group dedicated to identifying and documenting a transferable body of healthcare security metrics. The group is the result of a partnership between the Security Executive Council and the International Association of Healthcare Safety & Security (IAHSS).

“All departments are or should be encouraged to show their value and their return on investment in everything they do,” she says. “And though it’s very hard in our world to measure what we prevent or deter, there are a lot of ways security can show our cost efficiencies and our return on investment through data and other metrics that make it much more likely that we will be given the resources we need.”

“We have a fairly sophisticated incident software system that allows us to analyze and trend all incidents,” Michelman adds. The system allows for trending by building, day of the week, part of the campus, shift, and patient care unit. However, Michelman warns, the data from this system must be analyzed critically to be meaningful.

“If a workplace violence statistic goes up, for example, it may not mean there are more incidents occurring — it may mean that because of the extensive training we’ve done to encourage staff to report potential warning signs, people are reporting things they never would have reported before. So just because there’s a spike in certain types of statistics doesn’t mean you’re not succeeding; you just have to identify what the spike means.”

trained, educated, competent and committed security staff — really professional people who understand the complexities and nuances of healthcare. They should be compensated well and should have excellent benefits. You have to hire the right people for these jobs. This is a very complex environment, and you need very sophisticated skills.

“I look for people who are very smart, who have a compassionate side,” Michelman continues. “They must understand the state that people may be in. (I look for) people that are not easily flustered and don’t take things personally — because sometimes it’s not pleasant to deal with psych patients in the emergency department or upset visitors. I look for people with a strong ability to multitask and who have the ability to de-escalate people, who have negotiating skills and who are creative about understanding the types of risks we face.”

### Recognition of Hospitals as Soft Targets

While increased workplace violence is clearly on most hospitals’ minds, other trends have sometimes slipped under the radar. The terrorist threat is one of them. “Hospitals can be soft targets,” says Michelman, who is also a member of the Department of Homeland Security’s Advisory Council. “There are a lot of people in one place, and sometimes they are people others aren’t too happy with. They may be doing research in areas someone doesn’t agree with — there are radical groups against different types of research. Or there may be an individual or a domestic terrorist who believes a particular hospital was responsible for the death or severe injury of a family member.”

In addition, Warren says that hospitals play a crucial role in critical infrastructure, which heightens their target potential. “What happens if you have a bombing in your community followed by an attack on the hospital? That certainly limits your ability to treat the injured, and it adds to the psychological impact of a terrorist attack,” he says. Larger hospitals also contain equipment or radioactive source material that could be converted to weapons, he adds.

Planning for such events must be integrated into strong continuity plans, which all hospitals should test and maintain. “The best advice is to plan for an all-hazards approach, make sure all your plans, regardless of the source of the incident, can be put into effect, and make sure your plans are able to withstand any one of the many threats,” Warren says.

### Preventing Data Breaches

Another risk trend many hospitals have clearly left unaddressed or incomplete, is data loss. One might think that the longstanding HIPAA data protection rules would have by now prompted notable advances in the security of private health information, but that doesn’t seem to be the case.

Privacy Rights Clearinghouse ([www.privacyrights.org](http://www.privacyrights.org)) data shows that the healthcare industry suffered more reported information breaches in 2011 than any other industry category. Ponemon Institute’s Second Annual Benchmark Study on Patient Privacy & Data Security found that the number and frequency of data breaches in healthcare have risen, as has the number of records stolen or lost per breach. Employee mistakes, loss or theft of computing devices, and third-party errors were the three top causes of data breaches, the study found.



*“Workplace violence is part of an epidemic in healthcare now, and line staff must have at least a basic knowledge of how to recognize potential warning signs and how to react appropriately,”*

*says IAHSS president Bryan Warren.*

One of the faults often cited with HIPAA is that it lacked enforcement. In recent years, some fines have finally been levied, but they have been few and far between. In November, the Office of Civil rights began a program to audit up to 150 HIPAA-covered entities to “assess privacy and security compliance.” While it would be nice to say the potential of audits may impact hospital management to improve compliance, history has not borne out that hypothesis. What’s more, HIPAA compliance is clearly not the solution to the continued privacy breach problem.

HIPAA was not intended to be a security program in and of itself; yet, that is how many healthcare facilities have treated it. HIPAA compliance alone is no substitute for a fully developed, organization-specific protection plan that is built on the hospital’s unique threats, goals and culture. Non-compliance is a factor in the healthcare industry’s problem with privacy, but it is not the only one, and compliance alone is not the solution.

As the Ponemon study asserts, the majority of data loss events reported in healthcare occurred as a result of employee ignorance or neglect of proper protective actions. This could be corrected through appropriate, engaging training and an atmosphere that supports improvement rather than discipline alone. “We have a culture of transparency and not blame, so when someone is doing something that’s unhelpful from a security standpoint, we re-educate, we get people to ensure that they understand how to do things differently and understand what problem they may be creating rather than simply sanctioning them,” Michelman says.

Offering and mandating line staff training that is useful and effective is as important in preventing data breaches as it is in preventing workplace violence.

Active Shooter Training for Hospitals  
*SecurityInfoWatch.com and the IAHSS recently produced a webinar featuring 1 hour of training on handling active shooter incidents in your hospital. The archived webinar is available and free to view: <http://bit.ly/xNO7Zi>*

***“I look for people that are not easily flustered and don’t take things personally — because sometimes it’s not pleasant to deal with psych patients in the emergency department or upset visitors,” Michelman says.***

**A Shifting Business Model**

To compound all the continuing and growing risk issues hospitals face, the healthcare market is changing and hospital facilities are changing with

it. “The healthcare delivery system is shifting,” says Gibbs of Guidepost Solutions. “Instead of having a very large urban hospital with 1,000 beds, healthcare providers are building

Fiber Optic & Ethernet  
Network Solutions



**Don't let Your Transmission Equipment be the Weakest Link in Your Security Network**

The best-engineered security network is only as dependable as the transmission products you use. **Choose ComNet** for superior product performance, outstanding support and the best warranty in the industry.

**Turn to ComNet for Fiber Optic and Copper Transmission Solutions**  
Video – Audio – Data – Ethernet



**Choose ComNet...**

- The Industry's broadest line of Fiber Optic and Ethernet Transmission Products
- Environmentally Hardened for use in the Harshesst Environments
- Designed and Manufactured in the USA

**A Company That's Easy To Do Business With**

- Free Design Center Application Support
- Free Pre- and Post-Sale Technical Support provided by US Based Staff
- Lifetime Product Warranty
- “Customer is always right” attitude



**comnet**  
Communication Networks

For more information about ComNet and our complete line of connectivity and communication network solutions visit [www.comnet.net](http://www.comnet.net) or contact ComNet at [info@comnet.net](mailto:info@comnet.net) or call 203-796-5300 or Toll Free 1-888-678-9427

Visit Us at ISC West - Booth 3093



*“One of the keys to an effective security program is whether the designers of the facilities understand the concepts of crime prevention through environmental design (CPTED),” says David Gibbs, managing director of consultant Guidepost Solutions.*

regional clinics and 100-bed hospitals. In doing so, they are bringing healthcare treatment to the patient.”

The move to smaller, less centralized healthcare models has many drivers. It is a business decision to respond to the needs of patients and to make it easier for them to seek care. It is also a cost-based strategy — specialty clinics are far less expensive to construct and maintain than general hospitals, says Gibbs, particularly in places like the West Coast where OSHPD (Office of Statewide Healthcare and Planning Department) building seismic construction codes have a major impact on construction cost. And it’s a way to

add capacity to the healthcare system more quickly.

“As a result of all this, we’re seeing nationwide a strong interest in doing master planning, including security,” Gibbs says. “Hospitals need to re-assess how they do business. They need to look at their legacy way of addressing security — technology, physical spaces, etc. — by asking themselves, ‘are my employees safe and secure? Are my guests safe and secure? Are my patients safe and secure?’”

The projected healthcare building boom has another upside as well: It is likely to give more security teams input into building design on the ground floor.

“One of the keys to an effective security program is whether the designers of the facilities understand the concepts of crime prevention through environmental design (CPTED),” Gibbs asserts. “Architects are rarely trained in this topic in school. They often fail to understand that the addition of a wall, door, lock, gate, perimeter property vegetation berm, or an enclosed cage in the shipping /receiving department will have a major impact on the security program. If they attempt to add CPTED concepts later, not only will they impact construction costs, it may be impossible to change the design.” Guidepost Solutions conducts weekly presentations on CPTED for architects to help bridge this knowledge gap.

## The State of the Industry Is Promising

The challenges hospitals face are well documented, both inside and outside the industry. For this reason, responsible management is unable to remain unaware of the problems, and, says Warren, many hospital management teams are much more willing and

eager to address them. “Security has been a necessary evil for many years. But from an enterprise risk management philosophy, a lot of organizations are coming to appreciate the value-added services of security,” he says.

This will continue as security leaders like Michelman take creative approaches to adding value through their function. Massachusetts General works to minimize domestic violence-related injuries by offering services including home security assessments and assistance navigating court processes in order to press charges or file restraining orders. They also have a strong community policing model through which they send their own certified and trained personnel to do risk assessments of offsite facilities.

“I think doing those assessments and partnering with the people that work in those areas to look at strengths, weaknesses, recommendations for improvement and to prioritize implementing those improvements have really lowered the risk vulnerability and potential for criminal and unethical behavior to occur,” Michelman says.

Warren and Gibbs have seen a trend in management interest in moving security management to the network through implementation of IP equipment, for example. “Technology is wonderful—a force multiplier and a great tool — but you can’t rely on it alone,” Warren says. “You have to have well-trained, motivated security personnel, and you have to rely on your staff, because security is everyone’s responsibility. Everyone has to be the eyes and ears, and if the security culture of the organization is such that people understand what their responsibilities are, that’s really your best tool.” ■



Marleah Blades is Senior Editor for the Security Executive Council ([www.securityexecutivecouncil.com](http://www.securityexecutivecouncil.com)), a leading problem-solving research and services organization focused on helping businesses effectively manage and mitigate risk. For information, e-mail [contact@seclader.com](mailto:contact@seclader.com), or follow the Council on Facebook and Twitter.

**SECURITY TECHNOLOGY EXECUTIVE**  
**CUSTOM REPRINTS**

*Use reprints to maximize your marketing initiatives and strengthen your brand's value.*



**REPRINTS ARE IDEAL FOR:**

- New Product Announcements
- Sales Aid For Your Field Force
- PR Materials & Media Kits
- Direct Mail Enclosures
- Customer & Prospect Presentations
- Trade Shows/Promotional Events

---

For additional information, please contact Foster Printing Service, the official reprint provider for Security Technology Executive.

**FOSTER PRINTING SERVICE**

Call 800.875.3251 or [sales@fosterprinting.com](mailto:sales@fosterprinting.com)

