NOVEMBER/DECEMBER 2021

BEST PRACTICES:

HEALTHCARE SECURITY SUPPLEMENT

WHAT'S INSIDE:

A hospital relies on a strong, holistic security approach—and a little luck—to thwart a would-be shooter. Here are lessons learned from the experience. **Page 4**

Partnered Content:

Detex: Sneak Detection From The Door Hardware Experts **Page 3**

Partnered ads inside this issue:

Zbeta **Page 2**
Metro One **Page 5**
Garrett Metal Detectors **Page 12**

Photo illustrations by iStock

Killer requirements drive killer results.

When evaluating new technology initiatives and platforms for your physical security program, successful implementation depends on effective requirements. Learn how to choose the right systems and equipment at the onset, with the new ZBeta white paper.

Writing business objectives, mapping use cases and documenting critical features and functions is often overlooked in our field. When this is performed by people outside of the industry, the needs and nuances of your physical security mission can get lost. See how ZBeta delivers a well-tailored, targeted system of requirements that can drive stakeholder consensus, clarify what is essential, drastically reduce risk, and illuminate the path forward.

Download the white paper: zbeta.com/requirements

For product info #100 securitymgmt.hotims.com

ZBETA

Sneak Detection From The Door Hardware Experts

Detex puts dependable panic hardware in restricted secure areas - at building entrances, office entrances, and any other area where unauthorized entry must be controlled, and authorized entry must be easy, quick and reliable. You may also need to protect departments within your facility.

If your operation has certain entry doors where access must be limited to one identified entrant at a time, you want to be sure that no one is able to slip through undetected, behind an employee or vendor, during or after hours. Your restricted access system may be giving tailgaters an “enter free” pass. These unauthorized people can enter behind employees or members and cause problems ranging from loss of revenue to serious security issues.

You may also need to protect departments inside your facility. Member only fitness centers, corporate offices or record rooms must be off-limits to those who have no business there, and this hardware prevents unauthorized tailgate entry.

The Tailgate Detection System is compatible with most access control technologies, is easy to retrofit, and has an integrated door prop alarm for extra security.

Learn more about the restricted access system at *www.detex.com/sneak33*

MORE INFORMATION

Where Trust is Built™
DETEX®
Life Safety, Security and Security Assurance

Website: detex.com/sneak33

Phone Number: 1.800.729.3839

Email: marketing@detex.com

THE ACTIVE SHOOTER THAT WASN'T

A hospital relies on a strong, holistic security approach—and a little luck—to thwart a would-be shooter. Here are lessons learned from the experience.

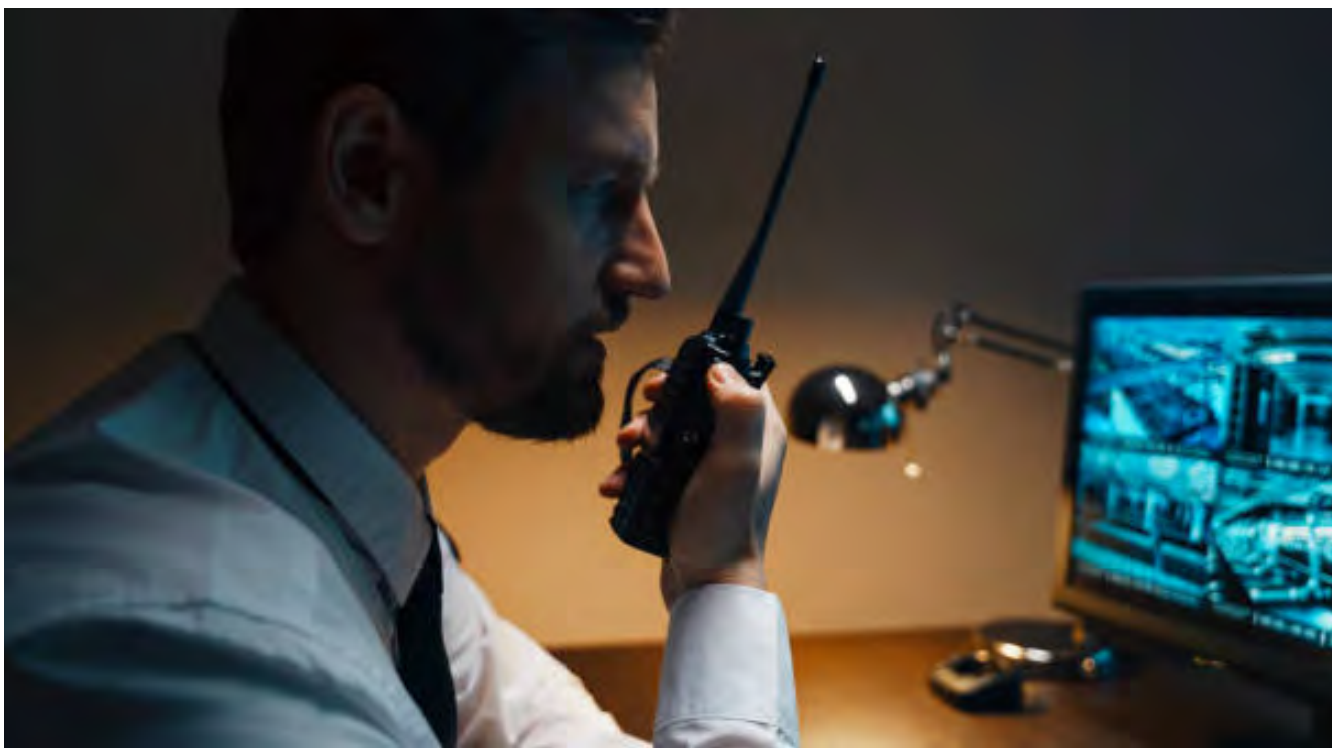
Eighteen minutes. On a sleepy Saturday morning in 2008, the actions taken in a span of 18 minutes were the difference between tragedy and just another sunny day in La Crosse, Wisconsin. Fortunately for the people at a mid-sized hospital there on 12 April, it ended up being just another sunny day.

But it wasn't entirely fortune. When Michael J. Barrett entered the hospital through an employee entrance carrying a concealed weapon, it wasn't fortune that led a cafeteria worker to notice something unusual, approach the man, affirm her suspicions that this was indeed unusual, and go straight to security to report it. That was security awareness training.

And yet, you can't help but think that fortune played a role. "There were things that went wrong," Drew Neckar, CPP, president of Security Advisors Consulting Group, said during a session at the recent Global Security Exchange (GSX) conference in Orlando, Florida. "But luckily, there were enough things that went right."

This is the story that Neckar, who was the midnight shift supervisor about to go off duty that morning, and his supervisor at the time, then security manager and now owner of NORD Security Management, Bob Nordby, CPP, told to the GSX audience at "Lessons from a Near Miss: The Active Shooter That Almost Was."

The overriding lesson: try not to overthink it. What saved the hospital that day was good, basic security practices. The lessons they learned—those "things that went wrong"—also were basic security principles. "In my role as a consultant, I see a lot of organizations place a lot of laser-like emphasis on countering the active shooter threat," Neckar said in an interview after the presentation. "It's important not to over-emphasize 18 minutes."



POSITION PAPER

Security Officers and Value-Based Pay

Security Officers are heroes, first responders, and life safety resources. They are professionals who deserve to be compensated commensurate with their contributions.

These highly trained men and women are required to protect our places of business, data centers, educational facilities, hospitals, and public gatherings. According to Metro One's President Joe Arwady, "If you can ignore the fictitious Hollywood stereotype of the bumbling, comical and inattentive security guard and instead picture real-life security personnel who daily protect lives and property, respond to emergencies, and keep us safe, it is logical to also recognize that these licensed, trained, and essential workers earn what we refer to as a "Living Wage," which is this case is synonymous with 'Value-Based Compensation'."

Consider the following numerical estimates from the U.S. Labor Department: Adult workers = 128.6 million; Law enforcement personnel = 696.6 thousand; and Private security officers = 1.2 million. In other words, one of every 100 workers in the United States is a private security officer, which in total represents roughly twice the number of public law enforcement personnel. Bottom Line: Private security officers are an essential commercial resource on which we rely for everything from directions inside a large office complex to saving a child's life by performing CPR.

As part of its ongoing commitment to corporate social responsibility, Metro One Loss Prevention Services Group has pledged to work with its partners to provide security employees with a living wage - - not based on government legislation but instead resulting from the value they generate for our society, institutions, and organizations.

The term "living wage" is often used to denote a wage that is enough to maintain a "viable" standard of living, in other words - - "the minimum." Metro One relies on Massachusetts Institute of Technology (MIT) and its Living Wage Calculator as one of several key measurement tools to establish viable wages for its security professionals. The Calculator is not a "security industry tool," but is universal, based on family size and the corresponding minimum levels of compensation needed to provide housing, food, clothing, health care, transportation, and childcare.

According to Arwady, the MIT relationship has helped position Metro One to advocate for compensation benchmarks that reflect the jobs and tasks assigned to its security personnel, a departure from the security industry's historical practice of "placing a guard for the lowest possible cost."

"Our service model recognizes the full value of our security personnel, starting with a living wage, but expanding total compensation, including health care and other benefits, to levels consistent with job requirements, risk and employee qualifications. Arwady says, "We believe it has brought us higher quality partnerships with our clients that stand the test of time and set a standard others can evaluate and hopefully embrace."

To be clear, both Neckar and Nordby are advocates for active assailant preparation and mitigation security measures. They emphasize that such measures need to be part of a comprehensive security approach that emphasizes actions, policies, and strategies appropriate to the risks faced by the organization.

Here's how that morning on 12 April played out.

- 7:35 a.m.: Man enters hospital through employee-only entrance. This is not detected at the time—it was discovered in video footage during post-incident review. (The 18-minute clock starts.)

- 7:40 a.m.: The man enters the hospital cafeteria area—bustling at this time in the morning—and stands near the back wall, observing. Again, this report is part of the post-incident review.

- 7:47 a.m.: At some point in the intervening minutes, a cafeteria worker notices the man, and it seems unusual to her. It did not seem like a threatening situation, so she walks up to the man and asks if she could help him with something. The man reaches for his belt and says, "I have a permit for this." The cafeteria worker disengages and proceeds to security.

- Approximately 7:49 a.m.: The cafeteria worker reports the incident to the security shift supervisor (Neckar), who instantly begins searching live video feeds to find the man. The supervisor radios the two security officers on duty, who leave their current posts and begin patrolling the hospital. The supervisor also calls 911 and reports that police may be needed at the hospital.

- 7:51 a.m.: Using video footage from high-traffic areas, the location of the suspect is narrowed down to a location on the fifth floor. That information is relayed to the security officers.

- 7:53 a.m.: A chaotic scene where the first security officer on the scene makes initial contact with the suspect telling him to remain still. Fortunately, the two security officers were approaching the location from different directions. As the suspect appeared again to go to his waist, the first security officer shouts "Gun,

gun, gun!" just as the security officer behind the suspect is able to initiate a takedown procedure. The 911 dispatcher is still on the phone, hearing the commotion, and urgently asking for details. The security officers report that the suspect is in custody. (The 18-minute clock ends. However, while the threat has been quashed, the incident—and the potential for lessons—is not over.)

- 7:55 a.m.: Police arrive in a flurry at emergency room waiting and demand to know how to get to the fifth floor. The receptionist is initially flustered and after a little back and forth, police are escorted to the fifth floor.

- Approximately 8:10 a.m.: Media begin to call, including national media. No senior hospital executives or communications staff are available yet.

There are many lessons and takeaways from these 18 minutes (and the immediate aftermath). Here's a look at some of those things that went wrong.

The first, obvious breakdown is access control at the employee-only entrance. The door was not locked down. Why? As Nordby said in the GSX session, "This was 100 percent convenience for the doctors." It's an obvious security weakness, but it was not an oversight. Prior to the incident, hospital leaders determined that the risk presented by the entrance was not severe enough to force badge access. Mostly, staff wanted to leave their badges in their lockers and not run the risk of forgetting them and being delayed access in the rare occasions when quick access was needed to prevent adverse patient reactions.

Another area of improvement was having an explicit process and training on what to do when police arrive during an emergency—no matter the time, since hospitals operate 24/7. It is easy to assume that absent other information, police will show up at emergency entrances, so additional procedures and training for that situation is called for.

A related lesson is that security did not have a public address system code for a situation where there was an incident that is no longer an emergency situation. They were still using the color system at the time. Post-incident, they initiated a more plain-language approach with an announcement starting with "security incident" followed by a specific condition or instruction.

Finally, the hospital's incident command system needed an overhaul as it was not up to the task for a significant Saturday morning incident. Communication channels and a system of on-call executives and communications needed to be established and tested.

Just as important is emphasizing what went right, and that starts with the hero of this story: the cafeteria worker. All hospital staff had been trained on security awareness, and to act when they feel something is out-of-the-ordinary.

"If that person hadn't noticed something and come told us, this could have been a very different incident," said Neckar. "We

wouldn't have had that five- or six-minute jump on it. It would have been a response to a shooting instead of a response to a suspicious person."

Some might question if it is wise to put a staffer in a potentially dangerous situation. Nordby explained that he thinks this situation occurred exactly as it should. If the person in question had been acting erratically or been doing something—anything—other than just standing there, then perhaps a direct report to security would have been in order. But 99 times out of 100, that initial customer service approach would have revealed that he was waiting for someone or needing direction of some kind. Instead it led to a concern, and the potential for danger, at which point the worker went straight to security. And that brings up the next success factor.

The next success factor is a combination of security planning and security drilling. Using crime prevention through environmental design (CPTED) principles, the hospital layout directed the flow of traffic in the hospital through choke

points, so these and other key entering and exit areas could be monitored by cameras.

The security drilling that came into practice was some gamification that the security team used in the control room in conjunction with officers on the floor—basically a game of hide-and-seek. This drilling, combined with the CPTED-influenced surveillance, is what enabled security to pinpoint the suspect's location in two minutes. The radio system worked as needed, and security officers were able to engage the suspect within two minutes of his location being identified. Next, security officer physical training meant the officers,—equipped with pepper spray, handcuffs, and keys, —were able to effectively take down a suspect who was carrying, but not yet wielding, a .44 Magnum handgun and hundreds of rounds of ammunition. And finally, there was a culture within the security team that they knew they were empowered to act. They knew that if somehow the takedown ended up being an inappropriate action, that, based on all the information the officers had at the time, it was a course that their supervisors would defend.

And do not completely discount fortune. That initial notice by the cafeteria worker coupled with the feeling that it just didn't look right? There's a bit of fortune in that. The approach from the security officers, when they were able to approach the suspect from different sides? There was no time to coordinate as they were still trying to sight the suspect. They just happened to be coming from different ends of the hospital. So really, it's great planning that allows you to capitalize on a little luck to prevent a tragedy.

A final point of emphasis from Nordby is to be sure to use major incidents to effect positive security change. "You don't want to appear to be opportunists," Nordby said. "But on the other hand, there are always security incidents happening, and when you have the attention of the executives, it's important to have a list of concrete solutions needed and examples to back up why the security measures you want to enact are necessary, and what the risks are if the measures are not adopted. When security is successful, nobody sees it, so it is important to document successes and share action reports."

SECURITY MANAGEMENT PODCAST

Enhance your ability to protect people, property, and information by listening to *Security Management Highlights*. Hosted by Chuck Harold, the monthly podcast provides practical solutions for navigating today's rapidly evolving risk landscape with interviews of security-industry leaders and *Security Management* editors.

Available on iTunes | SOUNDCLOUD

SECURITY MANAGEMENT

Wherever You Are

It's never been easier to access the vital knowledge you need to stay on the forefront of the security profession.

Receive timely information on emerging security threats and practical solutions through the channels that best fit your schedule and career.

MAGAZINE

Read the award-winning print publication from ASIS International.

WEB

Enjoy the latest news and a responsive design that looks great on your smartphone or tablet.

SOCIAL

Join the discussion on Facebook and Twitter.

PODCAST

Hear what security professionals are talking about.

EMAIL

Subscribe to the *SM Daily* and Deep Dive eNewsletters.

The NEW

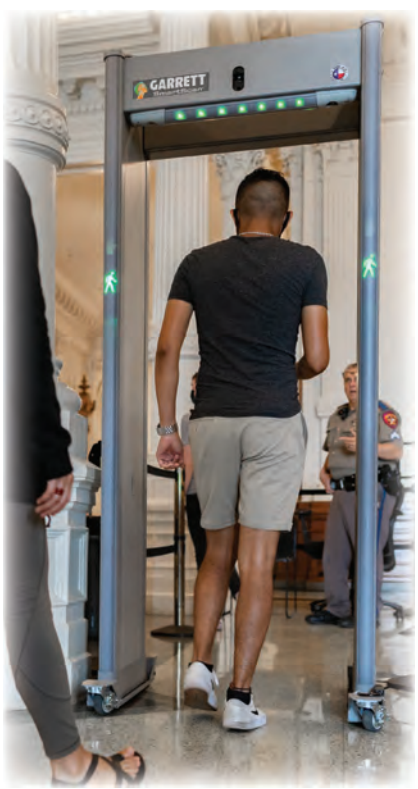
SMART CHOICE

GARRETT SmartScan THERMAL SCREENING SYSTEM

SmartScan™ Advantages

- Cost effective, fast temperature detection taken during normal screening operation
- Does not slow down existing screening process
- Battery-operated for ease of use
- Field upgradeable for any PD 6500i or Multi Zone with simple connections

MADE IN THE USA



GARRETT®
METAL DETECTORS

Email: security@garrett.com
Toll Free (U.S. and Canada) **800.234.6151**
Tel: **1.972.494.6151**

For more info: https://info.garrett.com/garrett-metal-detectors-smartscan

For product info #103 securitymgmt.hotims.com