The changing face of hospital security

Anthony Luizzo, PhD, CFE, CST, PI (Ret. NYPD), and Bernard J. Scaglione, CPP, CHPA, CHSP

To best combat violence at your facility, consider a range of technologies, from turnstiles to firearms and robots, and conduct cost-benefit analyses.

(Anthony Luizzo, Ph.D., CFE, CST, PI [ret. NYPD] is a member of the board of advisors for Vault Verify, LLC, in New Smyrna Beach, FL. He is a retired NYPD detective, the former Corporate Director of Security for the New York City Health and Hospital Corporation, a past president of the Society of Professional Investigators, and a former Eastern Region Governor of the Association of Certified Fraud Examiners. He is a former editorial advisory board member for Reuters WG&L/RIA Group - Thomson Publications. Luizzo is a member of IAHSS and a frequent contributor to this journal.)

(Bernard J. [Ben] Scaglione, CPP, CHPA, CHSP, is Principal of *The Secure Hospital,* a resource management and blogging site, and author of *Security Management for Healthcare: Proactive Event Prevention and Effective Resolution.* Scaglione, who has a master's in criminal justice, has served as security director for more than 25 years in NYC-area hospitals and has served IAHSS in several capacities, including on the Board of Directors. He is past Chairman of the ASIS International Healthcare Council and past President of the NYC Metropolitan Healthcare Safety and Security Directors Association. He is a frequent contributor to this journal.)

Our previous article in this journal furnished a roadmap for hospital security administrators to follow when evaluating their institution's readiness to handle future pandemic catastrophes [1]. This article focuses on increases in workplace violence and shootings and new threats that were not seen in the recent pre-pandemic world, such as civil unrest, staff strikes, and bomb threats from conspiracy theorists. The reactivation of previous threats and the advent of new threats arising from the pandemic should be a siren call to all healthcare protection professionals to take a second and third look at their institution's existing protection grid.

Pre-pandemic remediation strategies were not always effective in minimizing threats. Today, the ongoing and newer threats challenge healthcare security executives to leave the land of the familiar and begin seeking new

and more innovative protection blueprints, including security remedies that will handle any and all fast-coming threats. As we will discuss in detail below, sundry strategies to consider include conjoining in-house surveillance technologies with external public video systems, installing turnstiles, employing magnetometers, arming security personnel, incorporating robotics and drones in standard security machinations, and employing metrics to showcase proficiencies and substantiate expenditures.

To evaluate institutional crime risk exposure effectively, forward-thinking security executives turn to the security assessment for guidance. In competent hands, an assessment is analogous to a medical CT scan, a device used by medical experts to diagnose and treat illness. This risk assessment tool helps to diagnose and prescribe remedies for frail security programming while offering creative solutions to correct shortcomings before they wreak havoc on the institution. Additional information on preparing and effectively utilizing security assessments can be found in two articles authored by Luizzo [2] [3] and in the book mentioned in Scaglione's biographical note [4].

CONJOINING HOUSE AND PUBLIC SURVEILLANCE SYSTEMS

It makes good sense for healthcare security executives to reach out to local government and law enforcement officials to discuss joining the municipality's external surveillance network. Connecting to the community's surveillance network would permit the hospital security's eye-in-the-sky surveillance system to monitor access and capture mischievous activity and other noncriminal emergencies at the institution's periphery. Interestingly, on New Year's Eve a year ago, the New York City Police Department used both public surveillance and drones for the first time to monitor access control in Times Square.

Obviously, joining these existing networks would be a win-win for all in the never-ending war on terrorism. Conjoining surveillance technologies raises legal and logistical questions, but thinking beyond the standard way security projects are usually packaged could yield tremendous benefits.

TECHNOLOGICAL ENHANCEMENT CONSIDERATIONS

Turnstiles

Turnstiles, which were becoming more popular in the healthcare setting prior to the pandemic, provide a physical barrier between the entrance and the interior of the hospital. They also provide for the screening of everyone entering the hospital. Screening includes the authentication of all visitors and the issuance of an "access device," or pass, that enables entry into the hospital. The key to implementing a turnstile program is establishing reasonable security controls that adequately protect people, property, systems, equipment, and other assets while restricting access where appropriate. Ideally, program designers will consider internal traffic flow and its impact on clinical operations.

The screening process should be engineered to quickly maneuver traffic through the turnstile checkpoint as effortlessly as possible. It is therefore important that relevant signage be prominently posted and that security operatives be sensitized and briefed on how to keep visitors and staff moving freely without incident. The system should be capable of handling seniors and the disabled.

Keep in mind that some people will have difficulty with turnstiles and access control cards that require swiping for passing through. One obvious example would be a child accompanying a parent on a visit to a patient. Often, facilities will not be inclined to issue an access credential for the child, yet the youngster would have to pass through a turnstile. In this and other situations, human interaction will be required to assist those who do not understand or who have trouble navigating the barriers. Finally, some thought needs to be given to turnstile jumping and to illegal attempts to allow several people to gain access on the same card. We recommend that anti-passback programing be applied. An anti-passback system can be programmed to allow a credential to open a door or turnstile for a determined period so that an access card cannot be used by two different people.

Once the technological issues are addressed, it's time to tackle traffic flow. To get it right, you will want a traffic study that de-

termines high- and low-traffic periods and wait times. Once the new process is completed, it should be tested to ensure it will function flawlessly under extremely stressed circumstances and that the normal ebb and flow of the facility is not severely interrupted. For example, what happens when one or several of the turnstile portals malfunction? How will this downtime affect wait times? Will security staff be available to screen people when turnstiles are dysfunctional?

Costs must be considered as well. As with most technological enhancements, the higher the level of security one seeks, the costlier the system. Proximity cards, which do not require physical contact with a reader, cost the most. Should a less costly security technology be used, you will need to consider installing two or three different types of card readers or designating specific turnstiles for specific users, or both.

Most hospitals use proximity access cards for staff and less costly barcode or magnetic stripe cards for visitors and vendors. Obviously, budgetary considerations almost always drive the decision. Costs vary depending on whether the turnstile project is earmarked as a new construction or retrofit undertaking. A great many institutions engineer a system that offers a lane for visitors and patients, a separate lane for staff, and an additional lane for eventual breakdowns. Finally, let's not forget that an entry gate may be needed for deliveries and disabled access.

Magnetometers and Screening Procedures

In healthcare today, walk-through and handheld metal detectors are used primarily in emergency departments and in behavioral health areas. There is now interest in using metal detectors at hospital entrances. Protection wisdom theorizes that metal detectors and scan bag x-ray machines help to lessen the opportunity for illegal weaponry to find its way into healthcare facilities.

Before considering walk-through metal detection devices, survey the installation site, audit the detection device placement schematic, and evaluate its effect on access-related traffic flow. The court of protection wisdom holds that walk-through metal detectors should be placed in areas where it is possible for activation to restrict access and stop people from

bypassing the metal detector. Depending on traffic density, more than one detector may be needed to reduce wait times. We favor arming the security operatives who are assigned to monitor the detectors. In lieu of arming security staff, though, many hospitals install a physical barrier to obstruct entry at these strategic check points.

With respect to screening procedures, everyone entering the hospital should be scanned. The process should allow for handheld scanners so that any and all medical emergencies can be immediately adjudicated.

When metal detectors are used, all entrances into the hospital should be secured and monitored to make sure that no one wishing to enter the hospital can bypass the detection system. Finally, when metal detectors are used at emergency department entrances, a procedure must be implemented to handle individuals who arrive by ambulance but are not seeking medical treatment. Note that metal detectors are not effective if handbags, backpacks, and other carried items are not screened. These items should be sent through an x-ray machine or be physically inspected by a security operative. A table must be made available for inspecting bags. Initial inspections should *not* include a detailed review of a person's bags but simply a quick look-see for weaponry. If a weapon is suspected, security officers can use a handheld scanner to look for metal objects and, if need be, can conduct a full-blown inspection**.**

A private screening room needs to be erected to handle full-blown searches effectively. A process needs to be drafted speaking to what to do when a weapon is found. How will weaponry be safeguarded? How will legal weaponry be returned? Finally, a screening procedure is needed to handle special cases, such as infants and small children walking through detectors or arriving in a stroller and people who are in wheelchairs or otherwise physically impaired.

You will also need to attend to vendor, delivery, and law enforcement admittance. Procedures need to be drafted speaking to how bags or packages are to be searched. What will the process be for emergency personnel responding to an emergent situation? Will emergency responders be allowed to bypass the securi-

ty checkpoint without going through the metal detection? What will the process look like for on- and off-duty law enforcement personnel carrying firearms and other weapons? Finally, the trillion-dollar question: What is the policy when people refuse to go through the metal detector? Will service be refused, or will they be allowed to enter the hospital anyway? Questions abound!

Arming Hospital Security Operatives

In response to increases in active-assailant and workplace violence pre-pandemic, many hospital security directors moved to an armed in-house force. Whether to arm security personnel is an administrative decision that should not be taken lightly. Each institution needs to ponder it carefully, given that the choices made can have a major impact on the healthcare institution and its constituency.

Before arriving at a decision, hospital administrators need to decide on the purpose for arming security staff. Regardless of the reasons, the process must begin and end with getting legal advice and must include researching state and local ordinances and conducting a comprehensive risk assessment to validate the need for and impact of arming security personnel. Because of the high liability associated with arming staff, alternate approaches to having firearms on hospital property should also be pondered. Possible alternatives might include having an off-duty police officer assigned to the healthcare institution, hiring armed contracted private security, and arming only senior security management personnel.

If arming security is the road to be traveled, then the weapon of choice needs to be considered. When making that selection, questions galore arise. Among them: What type of revolver suits you best, such as single shot or semiautomatic, and if a semiautomatic firearm is deemed best, how large of a clip will be allowed? What type of bullet will be used? How much ammunition will be kept on site? Will the hospital purchase the weapons or ask officers to purchase the weapons out of their own money? If the former, will weapons be issued to each officer during shift changes? What will the ammunition carry policy entail? Prevailing security management opinion fa-

vors having the institution purchase all firearms and set the policy and standards.

With respect to safeguarding firearms, it is important that the institution provide an isolated and secure location for firearm storage. The room should provide a high level of security and have an ammunition cleaning area. The firearms storage room should have only one entrance and be equipped with a card reader and CCTV camera surveillance system. Access into the room should be restricted to *only qualified armed staff* who have a firearm issued to them.

A firearms instructor-supervisor position should be developed to keep track of all firearms, ammunition distribution, and collection. The supervisor should be an individual who has passed the certification program and possibly has prior law enforcement experience. A firearms supervisor should be assigned to each shift or work alternate shifts on a regular basis. Consider having a backup supervisor in addition to the supervisor who is selected.

Obviously if firearm use is added to the healthcare protection envelope, it is imperative to enact use-of-force guidelines. Issues to be considered include:

- state and municipal law requirements,
- type and amount of force to be used,
- whether aerosols or tasers will be allowed,
- training curriculum requirements,
- firearm type, distribution, and storage, and ammunition type, and
- training requirements and instructor availability.

Robotics and Drones

In a 2016 book, Robert J. Gordon, a professor in social sciences at Northwestern University, spoke of the possible use of robots in a wide variety of applications outside of the manufacturing and warehousing sectors, including supermarkets, doctor and dentist offices, and hospitals [5]. And, in 2019, James Vincent, writing for The Verge, noted that security robots are slowly becoming a more common sight in malls, and public spaces. What is more, these *friendly* robots are collecting far more data than humans could [6]! Obviously, robotics is becoming a part of the protection landscape and most

likely will play a much broader role in the years to come. It would be wise for security executives to put this new up-and-coming protection strategy on their radar screens.

In addition to using robotics, security executives need to network with local law enforcement agencies about the use of remote drone surveillance. According to an article by police captain Curt Fleming, 347 law enforcement agencies in 43 U.S. states are using unmanned aerial vehicle technology (drones) to assist in a wide variety of protection-related applications, including search and rescue, traffic control, surveillance, crowd monitoring, and active shooter investigations [7]. Ongoing synergism is especially important because hospitals play an extremely active role in terrorism-related occurrences, helping to treat the injured both during and after catastrophic occurrences.

FINANCIAL CONSIDERATIONS

Cost-Benefit Analyses

As with all security-enhancement endeavors, cost is always a major factor. Once the security scope of work is completed, it is time to consider preparing a cost-benefit study to compare intervention value against enhancement costs.

This analysis should consider both direct and indirect costs and benefits. Direct costs often include financial and operational costs associated with implementing proposed programmatic initiatives, and the indirect costs often involve productivity, business disruption, management-related diversion, loss of reputation, and brand value costs.

An excellent method of determining the amplitude of various security risk exposures is to subdivide identified risk exposures into *low, medium,* and *high* risk categories, listed in rows. Once the data is collected, add two columns with ratings of *vulnerability* and *criticality* in a matrix. It is through this analytic process that the amplitude of said exposures are valuated.

Further guidance on security risk evaluation can be found by contacting the International Association for Healthcare Security and Safety (IAHSS). IAHSS has published a set of basic guidelines to follow.

Applying Metrics to Validate Expenditures

Metrics is a management tool for measuring performance. Using metrics is an effective method of demonstrating security-related programmatic effectiveness and justifying expenditures. The two of us have written a trilogy of articles [8, 9, 10] highlighting several metric applications, and Scaglione's aforementioned book does the same. Using metrics helps the security executive speak the language that CFOs (bean-counters) understand. Moreover, using metrics is an extremely beneficial strategy to employ when seeking additional security enhancement dollars.

CONCLUSION

In today's world, the threat landscape is again changing, with increases in pre-pandemic threats and the advent of new, less conventional post-pandemic threats. One lesson from today's healthcare challenges is this: *If one is afraid to take chances, one can never get answers.* It is always good to be the "first to tomorrow" and begin embracing and experimenting with new security fixes. The techniques and technologies mentioned herein are only the tip of the iceberg but may be a good fit for your organization. Finding the right suit of armor to snugly fit your institution's wardrobe is not always an easy task, but wise security administrators have many advisors, both internal and external, to help them find the right protection attire for their institution's wardrobe!

References

1. Luizzo, A., & Scaglione, B. (2020). Disaster planning: Training for the perils of weapons of mass exposure. *Journal of Healthcare Protection Management, 36*(2), 1–10.

2. Luizzo, A. (2018, March/April). The security survey: An investigative tool. *PI Magazine, 156,* 28–30.

3. Luizzo, A. (2018, March/April). The security survey: An investigative tool – part II. *PI Magazine, 159,* 22–25.

4. Scaglione, B. (2019). *Security management for healthcare: Proactive event prevention and effective resolution.* Routledge/Productivity Press.

5. Gordon, R. J. (2016). *Rise and fall of American growth: U.S. standard of living since the Civil War.* Princeton University Press .

6. Vincent J. (2019, November 14). Security robots are mobile surveillance devices, not human replacements. *The Verge.* https://www.theverge.com/2019/11/14/20964584/knightscope-security-robot-guards-surveillance-devices-facial-recognition-numberplate-mobile-phone

7. Fleming, C. (2019). Remote drone dispatch: Law enforcement's future? *IACP Police Chief*

Magazine. https://www.policechiefmagazine.org/remote-drone-dispatch/

8. Luizzo, A., & Scaglione B. (2015). An alternative view in the development of security metrics. *Journal of Healthcare Protection Management, 31*(2), 98–104.

9. Luizzo, A., & Scaglione B. (2016). Resources available for applying metrics in security and safety programming. *Journal of Healthcare Protection Management, 32*(1), 27–33.

10. Luizzo, A. & Scaglione B. (2017). Applying metrics to 21st century healthcare security. *Journal of Healthcare Protection Management, 33*(2), 7–13.

Suggested readings

Luizzo, A., & Scaglione B. (2007). Training security officers to recognize the perils of weapons of mass destruction and pandemic flu contaminates. *Journal of Healthcare Protection Management, 23*(2), 1–9.

Luizzo, A., & Scaglione B. (2017). Aspects of crime and violence avoidance. *Journal of Healthcare Protection Management, 33*(1), 21–30.

Luizzo, A., & Scaglione B. (2019). Training security officers to recognize the perils of weapons of mass exposure contaminates – part II. *Journal of Healthcare Protection Management, 35,* 32–39.