What the C-Suite needs to know about the strategic value of a comprehensive security program

William S. Marcisz, JD, CPP, CHPA

The author provides the context that can help your administration understand the logic behind the design of your security program.

(William S. Marcisz, JD, CPP, CHPA, is President and Chief Consultant at Strategic Security Management Consulting, Inc., based in Apopka, FL. He is an expert in hospital and workplace violence security. He has 40 years of healthcare and legal experience and has assessed, developed, and implemented security and workplace violence programs in organizations ranging from small, rural hospitals to large, complex, multi-regional healthcare systems. He is a member of IAHSS. Reach him at William.Marcisz@SSMCSecurity.com.)

During the past 20 years, hospital and healthcare security programs have become more sophisticated and complex, primarily as a result of three drivers. First, security in healthcare is now highly regulated. Regulatory and accreditation agencies such as the National Fire Protection Agency (NFPA), the Centers for Medicare and Medicaid Services (CMS), and The Joint Commission, have created specific standards for how hospitals provide security and address workplace violence. Second, healthcare experiences a higher rate of workplace violence than any other industry. Finally, there are few true standalone hospitals left in the United States. Most hospitals are part of a healthcare system, which can range from large national enterprises with hundreds of hospitals and over 1,000 ambulatory care sites to small, one- or

two-hospital, organizations. Even small stand-alone hospitals have developed a network of local ambulatory care sites in their community.

To meet these challenges, healthcare security has evolved and become very professional. In medium-to-large healthcare systems, the senior security positions have evolved from security directors to vice presidents or chief security officers. Some command salaries in the $300,000–$500,000 range.

In working with healthcare facilities, I have seen that the organization's leadership is sometimes unaware of the ways the healthcare security field has changed to meet these challenges and of the strategic value of developing a comprehensive healthcare security program to ensure that regulations are met and top-quality security is provided. In this article, I outline some of the information that I share with these leaders, in the hope that it will be useful in your own efforts to gain support for your programs.

OVERALL PROGRAM DESIGN TODAY

Following the lead of large corporations, many healthcare security programs now use some variation of what may be considered a corporate security business model. Efficient hospital security programs are now designed around the following components: operations, communications, training, investigations, and physical security and technology. Other areas and business concepts from corporate security programs are also being deployed in healthcare security programs. These include enterprise risk management (ESRM), business continuity, crisis management, global security operations centers (GSOCs), threat analysis, and executive protection. And why not? Healthcare systems are merely corporations, with the only difference being that instead of protecting office buildings, manufacturing plants, or a network of commercial businesses, healthcare security professionals are tasked with providing security to a network of hospitals and care sites.

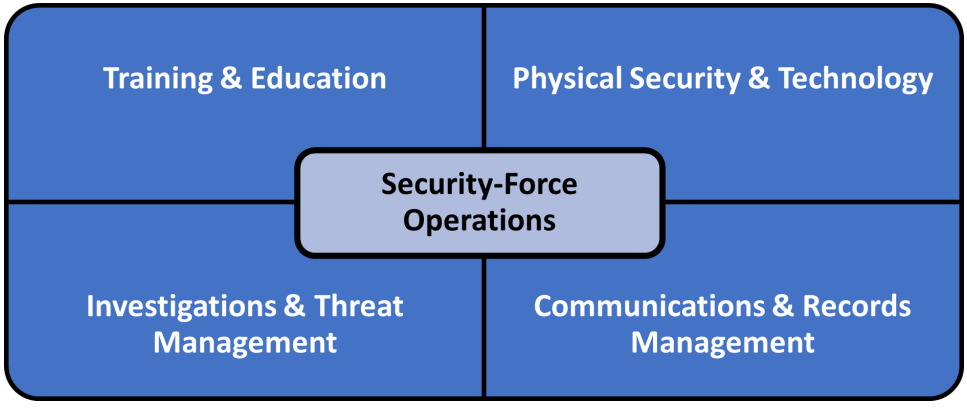
What differentiates healthcare security from corporate security is the need to address the high rate of workplace violence occurring at hospitals and the need for a large operations division (a

boots-on-the-ground uniformed security force). Corporate security programs tend to be built around investigations, threat management, and physical security—with operations, communications, and training viewed as support divisions. In healthcare security, by contrast, the focus of security administration is the operations division. The remaining divisions (physical security, training, communications, and investigations) tend to be developed internally to support the operations division (see the figure).

The dynamic in healthcare systems, particularly where hospital administrations have a high degree of autonomy, is that there is some level of competition for organizational, or "system," resources. Although the totality of the security program is considered a shared resource, the operations aspect of healthcare security in multi-hospital systems tends to be resourced locally at the hospital level, particularly when those sites are spread across a large geographic area. Many healthcare systems are finding that it makes sense for the remaining shared services functions of the security program (training, technology, communications, and investigations) to be administered at the system level, because these areas tend to require a higher level of subject matter expertise than the local hospital's security manager can provide for a site.

The system-based, shared security services model is of great benefit to the smaller hospitals in a system, because if they were

Healthcare Security Plan Components



a stand-alone facility, they could not resource a physical security professional, an investigator, a training manager, and a security operations center (SOC). When all the hospitals in a system pool resources, they can enjoy the benefit of having these subject matter experts available when needed.

Often, the difference between a good healthcare security program and one that is beset with challenges is an organizational understanding of security's role and that a minimal investment in security can create a return on investment or produce intangible value. A hospital's administration can, at times, present a barrier to the development of the organization's security program if it does not understand the benefit of the security operation or if the security leadership has difficulty explaining how a modern healthcare security program can be of value to the organization.

CONCEPTUALIZING THE SECURITY PROGRAM

A good way to explain the dynamics of an organizational security program is to break down the substance of the security program into two categories: "overt security" and "covert security." Both are required in a healthcare security program (The sidebar "Two Security Program Categories," lists the elements in each category.)

Overt Security

Overt security refers to the tangible and "seen" layers of a security program. In the context of a well-thought-out defense strategy, overt security measures can provide effective deterrence and response. Overt security mea-

Two Security Program Categories

Overt Security	Covert Security
Security Force Presence	Policies & Processes
Security Vehicles	Training & Education
Metal Detectors	Liability Avoidance/Risk Mitigation
Defensive Weapons (TASERs	Investigative Support
K-9's	Threat Management
Security Technology (CCTV, Duress)	Analytics/Artificial Intelligence
Visitor Management	Crime/Loss Prevention
Body Cameras	Drug Diversion Prevention
Lighting	Brand Protection
Physical Barriers	Business Continuity

sures tend to be those that can create a perception of safety.

Overt security measures are the easiest to gain resourcing for, but be aware that there is a downside to implementation if they are adopted in the absence of a clear strategic purpose for these measures and an understanding of how they fit into a multilayered security management plan.

Overt security measures should be implemented only when a security assessment indicates they are needed. They should not be implemented as a knee-jerk reaction to an adverse incident or to quell employee perceptions of safety issues. This is because overt security measures are generally the costliest in terms of implementation and sustainment. Although overt security measures can have value, their value does not always justify the cost of implementation, particularly if they create an unnecessary recurring annual expense.

In addition, overt security initiatives and practices can create unnecessary and unwarranted risk in some situations, as when introducing a security K-9 program at a site where there is little security risk. If you are trying to "make a splash" or take a shortcut to placate an unfounded perception of inadequate security or safety, you may well find that you have introduced a layer of security that adds nothing except added risk and unnecessary expense.

Finally, the implementation of an overt security measure can needlessly create liability exposure if a decision is later made to remove the measure (owing to it being unnecessary or not cost-effective) and an adverse incident occurs afterward. The plaintiff can use the implementation of the ultimately removed security measure as a basis to establish foreseeability that the environment was unsafe (otherwise, why would the hospital need the elevated security measure?). If the decision to remove the security measure was based on eliminating cost, this motivation compounds the difficulty of defending the hospital's position in a negligent-security claim.

Covert Security

Covert security is strategic and action oriented. Unlike overt security measures, covert measures can provide a discernable

return on investment and quantifiable value add. The difficulty of getting resources for the covert aspect of the security program is that people who are not security professions think of security in terms of optics, whereas a strategic security professional is more process focused. Strategic security management professionals merge the various overt and covert security concepts to design a multilayered security program that is a best fit for their organization.

Hospitals require a multilayered approach using both overt and covert security strategies.

The rationale for the overall plans that security leaders design will, of course, depend a great deal on knowledge of regulations and standards, yet I find that administrators and even some security directors—especially those who who are transitioning from law enforcement—sometimes are not as well versed in the regulatory demands and best practices as they should be. For instance, in some cases, security directors who were formerly in law enforcement and had done a good job in many regards in the development of the hospital's security program did not take healthcare regulations, or their organization's culture and mission, compassion, and empathy into consideration in establishing their programs. Some had not heard of the NFPA or did not know that the CMS forbids the use of handcuffs as restraints. In cases like these, I provide the information that follows.

UNDERSTANDING THE BROADER CONTEXT

A hospital security department cannot operate in a vacuum. The emerging standards and practices in healthcare security I alluded to earlier favor a multidisciplinary approach to providing a safe environment. A healthcare organization is best served if the security department is aligned with current hospital-based practices and guidelines. As an example, the trend toward employing a multidisciplinary approach to workplace violence prevention is now a Joint Commission requirement (see LD. 03.01.01 EP 9) [1].

The evolution of healthcare security has been driven to a great extent by an increase in workplace violence and a need to standardize strategies, prac-

tices, and technologies that have been developed to prevent and respond to the ongoing epidemic of workplace violence.

Several regulatory agencies with healthcare industry oversight have stepped in and created standards, requirements, and guidelines centering on hospital security and workplace violence prevention. In addition to the CMS, TJC, and NFPA, these include Det Norske Veritas (DNV), and the U.S. Occupational Safety and Health Administration (OSHA), as well as many state-level agencies.

In addition, healthcare trade associations such as the Emergency Nurses Association (ENA), the American Society for Healthcare Risk Management (ASHRM), the American College of Healthcare Executives (ACHE), the American Hospital Association (AHA), and the American Society for Healthcare Engineering (ASHE) have all weighed in on best practices for healthcare security and workplace violence prevention in healthcare.

What is more, the American Society for Industrial Security (ASIS) has partnered with the Society of Human Resource Management (SHRM) to create formal standards on workplace violence prevention and threat management.

In working with clients, I routinely urge them to join the IAHSS, which, as readers of this journal know, is dedicated to formally and informally sharing information about compliance and best practices and advancing the field's professionalism. I inform clients that IAHSS has partnered and collaborated with several other professional healthcare industry trade organizations and has developed dozens of healthcare security guidelines and best practices using a multidisciplinary approach. Considering that IAHSS is partnering with other hospital trade organizations (such as those listed above) and that those trade organizations look to IAHSS to provide best practices for healthcare security, it makes sense for a hospital security team to be aligned with IAHSS guidelines. This alignment will help to position the team well for when a stakeholder leader from human resources, risk management, or the administration seeks advice on how best to provide security in certain areas of the hospital.

IAHSS guidelines provide security solutions and the framework for security program development. Membership in the organization also provides the added benefit of enabling members to network and develop relationships with other hospital security directors and managers, who can offer feedback about what may or may not work in relation to procedures, equipment, technology solutions, and other aspects of how best to provide security in a hospital. Borrowing a catch phrase from the New York State Lottery, "You've gotta be in it, to win it."

CLOSING COMMENT

Healthcare security has come very far very quickly in response to changes in the delivery of healthcare services. Staying ahead of the curve requires a strategic approach and planning to align your security program to the healthcare system's business plan. More importantly, to get to their destination, savvy security directors must know how to communicate the value of security to an administration that may not understand the value or strategic importance of security in the organization. I hope this article has been a helpful in assisting you to educate your organization's leadership about what healthcare security is and how it can be employed to not only create a safer environment in care facilities but to also contribute to increasing business efficiencies and reducing risk.

References

1. Marcisz, W. S. (2022, August). Understanding The Joint Commission's requirements for workplace violence prevention. *Journal of Healthcare Protection Management, 38*(2), 10–22.