Guidepost

IS YOUR SECURITY VULNERABILITY ASSESSMENT A PART OF THE REQUIRED HAZARD VULNERABILITY ANALYSIS – THOUGHTS FOR HEALTHCARE PROVIDER ORGANIZATIONS

For nearly twenty years, since the events of September 11, 2001, the U.S. Departments of Health and Human Services and Homeland Security have encouraged and funded efforts by healthcare organizations to expand their emergency response plans and overall readiness for disasters. With the same goal in mind, The Joint Commission ("TJC"), the nation's oldest and largest standards-setting and accrediting body in health care, introduced new emergency management standards that require hospital emergency response plans be based on a hazard vulnerability analysis ("HVA") performed by the hospital. TJC defines HVA as "the identification of hazards and the direct and indirect effects these hazards may have on the hospital." While the standards were updated two decades ago, TJC has not formalized the process for conducting an HVA nor has it offered a specific tool to normalize the process within hospitals. Several models have been developed and circulated but most are simple spreadsheets where a relative risk rating is calculated based upon known threats, probability, vulnerability, and perceived severity (magnitude-mitigation).

Generally, the HVA is completed annually by an organization's Environment of Care committee. An HVA is designed to aid in preparedness and mitigation activities under an "all hazards" approach. Security vulnerabilities are a subset of the more broad and inclusive hazards a healthcare organization may face and are commonly considered a part of the risk or emergency management function's responsibilities. A healthcare organization faces many types of risk, most of which are incident driven such as active assailant, bomb threat, civil unrest, forensic admissions, hostage situations, suicide, weapons, theft, assault, abduction, vandalism, fire, flood, earthquake, tornado, utility failures, and other

natural disasters.

Local priorities that are based solely upon opinion, and not objective data, can provide a weak basis for planning and preparation. Expert opinions from clinical or administrative staff in an HVA can result in a waste of time, duplication, missed opportunities, siloing, and confusion over the true priorities in terms of threat, vulnerability, and risk. The potential incidents of manmade/criminal acts are more directly the responsibility of the security program and are more appropriately documented and evaluated through the completion of a Security Vulnerability Assessment ("SVA"). An SVA includes addressing the approximately 20 basic security risks a healthcare organization may face.

The Timing of the SVA

The identification of specific security risks, their magnitude, and potential impact on the healthcare organization is but the initial step in protecting the organization. An SVA should be conducted every three years or any time a major change in operations or physical conditions have transpired. The objective is to identify any security exposures so that a comprehensive security plan can be formulated and implemented. Evaluating the security program in its entirety (operations, management, and technology) and developing recommendations for solutions as opportunities for strengthening the overall security program is the deliverable for this type of assessment.

Although TJC does not limit the HVA to a hospital's campus in the requirement for annual HVAs, many healthcare provider organizations omit offsite locations and clinics in their assessment. This is a mistake that can easily be illustrated by the recent shooting in a Minnesota medical clinic leaving one dead and at least four injured, three critically. The shooter was unhappy with the care he received and sought vengeance.

Conducting the SVA – Two Approaches

The manager or director of security generally provides the information for the SVA to be incorporated into the HVA on an annual basis. Given that security vulnerabilities are manmade/criminal incidents, the information should be readily available and easily found within the security department's incident reports. The evaluation of the security program as a whole — evaluating mitigation capabilities through an SVA — is much more complicated. This leads to the question of who best should conduct the assessment.

The first approach is to have the person with responsibility for day-to-day security operations, such as the security manager or director, conduct the SVA. This security professional should have (1) general knowledge of the organizational structure and philosophy, (2) the community's assessment in terms of criminal activity, the surrounding environment, and past problems, and (3) access to department heads and supervisors, all of whom can provide candid feedback about their experiences. The two main areas of concern with this approach are (1) does the individual have the qualifications to conduct an SVA, and (2) the potential for implicit bias or lack of criticality when evaluating one's own program. Merely being in a position does not in itself qualify an individual to conduct a valid SVA. A qualified professional will possess a certain level of education as well as experience within the hospital setting. Such

qualification is often validated by trade associations such as the designation of a Certified Healthcare Protection Administrator (CHPA) conferred by the International Association for Hospital Security and Safety (IAHSS) or that of a Certified Protection Professional (CPP) conferred by the Professional Certification Board of ASIS International. Involving a person with these credentials or experience in security, safety, or risk management for more than one healthcare provider organization is recommended.

The second approach is to engage an outside security consultant who brings the experience and credentials outlined above. In addition to these bona fides, an advantage to engaging an outside consultant is that this professional comes to the assessment with an objective viewpoint, something that may be difficult for the security manager or director with daily oversight responsibility for the program. Additionally, a consultant can generally perform the assessment in a more efficient manner by bringing to the assessment a body of healthcare sector operational expertise and a broad range of solutions from which to draw based on past experience.

Whichever route you take; it is important for healthcare provider organizations to consider an SVA as a critical part of the HVA process required by TJC.

TIMOTHY SUTTON CPP, CHPA, PSP

Senior Security Consultant

Timothy Sutton has more than 30 years of security experience. His expertise includes operational security management and program development, loss prevention, physical security and risk assessments, and technical security systems design and implementation. He has worked with clients in diverse sectors including medicinal and adult-use cannabis, healthcare, retail, government, manufacturing, and multi-use properties.