

Vulnerability and Risk Assessments

In the Environment of Care

Karim H. Vellani, CPP, CSC and Robert E. Owles, CSC



2007

Vulnerabilities are opportunities, opportunities for crime, opportunities for rule breaking violations, opportunities for loss. By definition, a vulnerability is a weakness or gap in a security program that can be exploited by threats to gain unauthorized access to an asset. Vulnerabilities include structural, procedural, electronic, human and other elements which provide opportunities to attack assets.¹ While healthcare security professionals continue to update and expand their threat assessments with events such as natural disasters, avian flu, and terrorism, the primary threats that continue to impact hospital assets include ordinary crimes, unauthorized access, and patient abduction. For all of these threats and others, the vulnerability assessment's objectives are to maximize life safety, protect assets, and maintain continuity of operations. To meet these objectives, a comprehensive and robust security program must be in place to address the known and unknown threats that exist both outside the hospital's facilities, and also inside. The Joint Commission's standards² require that hospitals identify and manage security risks. A key component of that identification process is a vulnerability assessment.

Vulnerability Assessments

A vulnerability assessment is a systematic approach used to assess a hospital's security posture, analyze the effectiveness of the existing security program, and identify security weaknesses. The basic process of a vulnerability assessment first determines what assets are in need of protection by the facility's security program, then identifies the protection measures already in place to secure those assets and what gaps in protection exist. Finally, the assessment measures the security program's effectiveness against valid security metrics and provides recommendations to security decision makers for improvements. In essence, the vulnerability assessment assists hospital security decision makers in determining the need for additional security systems, equipment upgrades, policy and procedure revisions, training opportunities, and manpower needs.

Vulnerability assessments identify security weaknesses that can be exploited by an adversary to gain access to the healthcare organization's assets. For example, a vulnerability assessment may reveal an egress path that could be exploited by an infant abductor or it may identify a lack of patrols by security personnel in sensitive areas of the hospital. The goal of vulnerability assessments is to ensure life safety, protect assets, and the continuity of operations. The driving forces behind vulnerability assessments include new legislation or regulatory requirements, Joint Commission guidelines, revised threat assessments with new or emerging threats, increased criticality of assets, and the construction of new facilities on a hospital campus. For example, the recent infant abduction from a Lubbock, Texas hospital or the sexual assault of a patient in a California hospital prompted other hospitals to perform a vulnerability assessment of their own hospital to ensure adequate security in these areas.

The vulnerability of an asset is determined by the potential weaknesses in operational processes and procedures, physical security weaknesses, and technical gaps which can be exploited to attack an asset. Vulnerability assessments are used to identify these weaknesses by way of a security survey. A security survey is a fact-finding process whereby the assessment team gathers data that reflects the *who, what, how, where, when, and why* of a hospital's existing security operations³. The purpose of a security survey is to measure the vulnerabilities at a facility or to specific assets by determining what opportunities exist to exploit current security policies and procedures, physical security equipment, and security personnel.

Security surveys are simply questions and checklists that must be completed by the assessment team during off-site preparations and on-site inspections of the facility. Surveys may range from a few basic questions to highly detailed lists comprising thousands of questions. A typical security survey contains general information about a site and evaluates the geographic characteristics of the hospital's facilities, physical layout of each facility and its unique characteristics, security personnel and deployment schedules, operational requirements, security equipment capability, and other items that impact security. Security surveys are designed to meet the unique needs of a facility or type of facility. Even within similar types of hospitals, unique characteristics must be considered and included in the security survey. General information normally captured in a security survey includes:

- Vulnerability Assessment Team (identified by name and title)
- Names, addresses, and descriptions of the Hospital's buildings and its support facilities (patient care building, clinics, research labs, etc)
- Number of Floors
- Bed Count
- Campus size and location
- Normal Operating hours for each facility
- High activity use (hours/days)
- Individuals who have access to security sensitive areas
- Location of critical assets within each facility
- Known vulnerabilities at each facility
- Identification of building systems, such as mechanical, communications, HVAC, water, electrical, medical gas, etc.

The security survey checklist should also consider specific information such as organizational issues such as the hospital's culture, visitor management practices, security force utilization, and emergency preparedness. Life safety practices and systems must also be considered in context with existing and conceptual threats, particularly those that affect patient safety. Asset specific vulnerabilities are also included in the security survey. For example, if the hospital has research labs, protection systems and personnel are typically employed for lab and information protection. Likewise, emergency centers create many opportunities for crime and rule violations and require special attention. Threat types and frequency in the emergency center may be different from the rest of the hospital's facilities.

Office area security and loading docks are also at the forefront of most security directors and managers. Administrative offices are likely to experience wandering people, purse thefts, and loss of business equipment. In this regard, it is important to consider the culture and practices of administrative personnel. Are doors locked when an office is unoccupied? Are purses stored in locked drawers? Recurring security awareness training is often an effective and inexpensive solution for office area security problems.

Loading docks serve as a primary gateway for would-be offenders as they are often left open and unattended. Valuable assets, such as computers, are sometimes stored on the dock for extended periods of time. The problem is compounded when dock personnel are short staffed or inattentive. Worse yet, dock personnel may be complicit in theft of hospital property. Penetration tests of loading docks often yield surprising results about the vulnerability of hospital assets. Properly securing the loading docks is a critical element of an effective security program.

Notable security survey areas to consider for each building include:

- Perimeter Barriers and Controls
- Vehicle Control and Perimeter Entry Point Access
- Clear Zones and Signage
- Building Exteriors
- Access Control and Visitor Management
- Lock and Key Control
- Outdoor Lighting
- Closed Circuit Television (CCTV)
- Intrusion Alarms

- Architectural Design and Crime Prevention Through Environmental Design (CPTED)
- Patient/Infant Abduction Systems

Once all areas of the buildings have been surveyed by the vulnerability assessment team, outside areas should be assessed. These areas may include small parks or courtyards, smoking areas, and parking facilities. For each of these areas, the survey should address access control, personnel (security, parking attendants), lighting, physical security measures and systems, and architectural design. As one of the few objective areas of a vulnerability assessment, lighting in particular is often found to be a measure in need of enhancement to improve the overall strength of the security program and reduce the fear of crime.

Asset-Based and Threat-Based Vulnerability Assessments

As stated above, vulnerability assessments is a process used to identify weaknesses or gaps in a security program that can be exploited by threats to gain unauthorized access to an asset. While vulnerability assessments are generally conducted using the same general process, the manner in which they are conducted may change based on the focus of the vulnerability assessment team. For example, the vulnerability assessment team may focus on specific assets, such as people (patients, employees, etc) when conducting the assessment. On the other hand, the team may focus on specific threats, such as patient abduction, when walking through the security survey. The focus of the team determines whether the vulnerability assessment is asset-based or threat-based.

Asset-based vulnerability assessments are broad evaluations of assets and the threats that impact those assets. For example, an asset-based assessment at a hospital's research lab will focus on the information developed by the researchers, both from a physical security and information security perspective. In this instance, the primary asset in need of protection is the information in both its physical form (computers, paper, etc) and its electronic form (software, files, etc). Asset-based assessments assume that every scenario cannot be imagined or those that are, are too speculative to consider. By in large, asset-based scenarios are the most common type of assessment utilized by security practitioners today.

Threat-based vulnerability assessments, on the other hand, focus on the various types of threats that challenge hospital security practitioners. More often than not, the threats considered are those that are low frequency, high impact, such as infant abduction, patient sexual assaults, and city- and region-wide emergencies such as hurricanes or terrorist acts. The threat-based assessment evaluates vulnerability by asking how a patient may be abducted, how prepared the hospital if supply chains are cut off for an extended period of time, or how the loss of utilities will impact patient care. This type of assessment requires a knowledgeable assessment team who has an understanding of

historical events at hospitals and has the ability to foresee future events, especially conceptual threats. While history is a primary indicator, not all future threats can be anticipated based on the past attack modes. Conceptual threats should not be underestimated. Scenario-based assessments are advantageous in that they are better suited for assessing high value assets and high consequence threats. Unfortunately, this advantage also creates a problem whereby lesser threats may be ignored and security measures not implemented.

While the vulnerability assessment team's goal is to select a low frequency threat for the assessment, the scenario must be sufficiently realistic. A fair assessment of the asset's attractiveness, from the adversary's (threat) perspective, is critical to accurately evaluate the strengths and weaknesses of each asset and the security program. The next step is to evaluate the ability of the existing security program to deter, detect, and delay an attack. Typically, an outside - in approach is used whereby the vulnerability assessment team identifies the outer most layer of protection and works their way inside toward the assets, passing thru each security layer in the same order that an adversary would do so. The training, skills, and equipment of the theoretical adversary should be considered as each protection layer is breached. Finally, the assessment team analyzes the consequences of the threat reaching its target and assigns a vulnerability rating.

An example of a scenario-based vulnerability assessment is where the assessment team selects a low grade explosion outside a patient care building as an attack scenario. They postulate that the explosion occurs immediately outside the building during daytime hours. What are the characteristics of the building and its assets (patients, families, employees) that may contribute to the loss, damage, or destruction. How would an attacker detonate a bomb in close proximity to the building? Would any element of the current security system be able to deter, detect or delay the attack? Would the closed circuit television (CCTV) system detect the adversaries? Is the CCTV system monitored with direct communications to the security response force? Would the building survive a low grade explosive attack?

As seen in this example, a downside to scenario-based assessments is evident, in that these types of assessments force the team to focus on protecting against particular threats and potentially ignoring other threats. Nevertheless, both asset-based and threat-based vulnerability assessments are beneficial exercises that should be undertaken on a regular basis. The results often yield relevant solutions and also identify opportunities for training emergency responders and security personnel.

Vulnerability Assessment Results

The outcome of a vulnerability assessment and security survey is set of recommendations geared toward closing gaps, mitigating risks, and improving the security program. In large hospitals, the recommendations may be phased or prioritized based on cost and mitigation strength, the ability for the recommendation to reduce risk.

Risk reduction recommendations typically fall into one of three areas: policies and procedures, physical security measures, and personnel. Policies and procedures may include revising the hospital's security management plan, security awareness training, or revising procedures that reduce crime opportunities, such as implementing a buddy system. Policies and procedures also define how the hospital responds to sentinel events and the methods use to reduce the adverse impact to the hospital and its assets. Physical security improvements may include such things as redesigning facilities or areas to increase pedestrian or vehicular traffic, installing an electronic visitor management and access control system, or connecting duress alarms to a central station. Because many hospital security departments are in a constant state of improvement, electronic security measures must be scalable and expandable in anticipation of future growth. Security personnel recommendations may include additional training, better equipment, or stronger supervision. Hospitals which utilize a security force be it proprietary, contractual, or comprised of law enforcement officers, know that some of the greatest areas for security program improvement lie with the security force.

The Decision Maker's Challenge - Post Risk Assessment

Once the vulnerability assessment is complete and coupled with the threat assessment, the final risk assessment report is ready for action. The challenge for the security decision maker is to assimilate the data into a meaningful security plan that will address the weaknesses and exemplify the strengths of the organization.

The initial review of the risk assessment report is critical. The security management team must thoroughly review the risk assessment report and validate the findings and recommendations. This procedure focuses on actual observations, data, and other available material to clearly understand the intent and magnitude of each finding and recommendation. During the process, the modification of a finding or recommendation could possibly reveal other opportunities. Adding or deleting certain information helps to clarify the specific problem and strengthen the recommendation. The intent is not to hide or delude the finding but to ensure that the identified measure, process, or program receives appropriate attention and implementation if required. For example, a particular finding might address inadequate staffing at a point entry after hours. The subsequent recommendation states that the post requires a security officer at the entry point between the hours of 7:00 p.m. and 6:00 a.m. seven days per week. Subsequent analysis discloses the door is secure during those hours and observed by a camera. However, while analyzing the problem further management recognizes a need for an officer during normal business hours. Consequently, the modification of the finding and recommendation better identifies and addresses the actual security shortcoming. This example is more elaborate than most modifications, which generally entails wordsmithing or adding more detail to the finding and recommendation. It is imperative that weaknesses are clarified and validated in order to appropriately apply solutions for the short- and long-term. Further, weaknesses need to be categorized, prioritized, and

analyzed to determine criticality, economic considerations, implementation timelines, and to what extent.

Following the review process, security management should coordinate with risk management, safety, and possibly with emergency management, providing them a copy of the risk assessment report. A thorough review and discussion of the findings and recommendations with these departments is not only appropriate, but will prove to be extremely beneficial. The security risk assessment is a process that examines the health care organization from a holistic perspective and the findings and recommendations have a broad application throughout the organization. Sharing the security risk assessment with risk management, safety, and emergency management actually puts security management in the driver's seat when presenting the findings and recommendations to senior management. The support of these departments is critical should funding be required to implement some of the recommendations. Risk management coordination assists in alleviating legal issues associated with some of the recommendations, which is prudent and crucial for the maintaining a viable security program. Safety, on the other hand, assists with recommendations requiring special knowledge of sophisticated medical applications and procedures that are associated with one or more of the security recommendations. The emergency management coordination and review offers valuable insight into how emergency incidents and events might require a different approach to one or more recommendations. Coordination with the aforementioned departments may be obvious. However, there are many others to coordinate with, such as Information Services (IS). Recommendations that require the implementation of sophisticated technology hardware and software definitely requires IS coordination. Another example, is nursing operations. The impact on patient care areas, resulting from a risk assessment, such as waiting areas, surgery areas, pharmacies, and specialized clinics, is common. Coordination with the nursing leadership assists in assuring a smooth implementation process. The examples given are just a few of the considerations that must take place while preparing to implement the recommendations. Nonetheless, once the security risk assessment review and analysis process is complete, briefing senior management is the next challenge.

Senior Leadership Briefing and Capital Funding

Security management has the inherent responsibility to provide an accurate and timely report to senior management. The security team's thorough analysis and the presentation of sound recommendations is the next step. Preparing for this task begins the day the assessment is completed. All the coordination and analysis must produce a sound plan and timetable for implementing the recommendations. Additionally, a cost analysis must clearly depict the potential cost associated with recommendations requiring funding for implementation. The presentation must be an executive summary, with enough detail to support the recommendations and the implementation plan. However, it is vitally important for the senior security manager to be prepared to answer

questions in greater detail if required. Once the plan is approved, partially or in full, the next step is acquiring the necessary funding.

Coordination with business services immediately following approval is paramount to acquiring capital funding in a timely manner. The organization's financial services group assists with preparing the capital funding request and the method of presentation to the Capital Projects Committee (CPC).

Implementation of Recommendations

Following the security risk assessment presentation to the executives, and while preparing the capital-funding request, the implementation of the remaining approved recommendations, in accordance with the implementation plan, begins. It is imperative not to delay the implementation of the recommendations, because the organization remains at risk.

The security risk assessment is an extremely valuable process. The security manager can use the assessment to leverage support for the security program, acquire crucial funding, and have the ability to implement timely improvements to bolster the organization's security posture. Furthermore, the security manager has a perfect opportunity to emphasize the strengths of the security department and promote the risk assessment as a proactive approach to enhance the organization's security posture.

ABOUT THE AUTHORS

Robert E. Owles, Jr. is the Director, Security Services, at Texas Children's Hospital, where he is responsible for a large, diversified security operation that keeps pace with the hospital's challenging strategic objectives, in a dynamic health care industry. He is a member of the American Society for Industrial Security (ASIS-International), the Association of Certified Fraud Examiners (ACFE), and the International Association of Healthcare Security and Safety (IAHSS), serving currently as the Chair of the Houston IAHSS Chapter. Bob holds a Bachelor of Science degree in Business Management from LeTourneau University, a Master of Arts degree in Organizational Management from University of Phoenix, and is currently pursuing a second master's degree, an MBA in Health Care Administration.

Karim H. Vellani, CPP, CSC is the President of Threat Analysis Group, LLC, an independent security consulting firm. He is Board Certified in Security Management and a Certified Independent Security Consultant. Karim is a member of the International Association for Healthcare Security & Safety, the American Society for Industrial Security (ASIS-International), and the International Association of Professional Security Consultants, serving currently as the Vice President. As an independent

security consultant, Karim has extensive experience in risk and security management in the healthcare industry and has written extensively on the subject. He has also authored two books, Applied Crime Analysis and Strategic Security Management. Karim can be reached via email at kv@threatanalysis.com or via phone at (281) 494-1515.

¹ Vellani, Karim H. (2006). Strategic Security Management: A Risk Assessment Guide for Decision Makers. Woburn: Butterworth-Heinemann.

² Joint Commission on Accreditation of Healthcare Organizations (2005). Environment of Care Standard 2.10.

³ Sennewald, Charles A. (2003). Effective Security Management, 4th Edition. Woburn: Butterworth-Heinemann.