Strategic Security Management: Risk Assessments in the Environment of Care

Karim H. Vellani, CPP, CSC

Securing the environment of care is a challenging and continual effort for most healthcare security managers, who face unique challenges in balancing the open campus environment with the protection needs of the hospital's patients, employees, and other assets. No hospital is without risk and effectively managing risk is crucial to maintaining the protection and openness balance. By conducting a comprehensive risk assessment, hospital security managers can prioritize identified risks, develop an effective hospital security program, and reduce risk to a manageable and acceptable level. This article discusses a 5-step risk assessment process that enhances the hospital security program by effectively mitigating risks to the hospital.

Risk management, as the name implies, is the management of risks to an organization. For most healthcare facilities, risk management includes not only security functions, but also insurance, legal issues, and health and safety. The primary component of risk management is the risk assessment process whereby risks are monitored and addressed on a continual basis. This process consists of the identification of threats, vulnerabilities, and risks to the hospital with the end goal of selecting appropriate security measures to reduce identified risks. As seen in the flow chart below, the five steps of the risk assessment process are asset identification, security inventory, threat assessment, vulnerability assessment, and risk assessment.

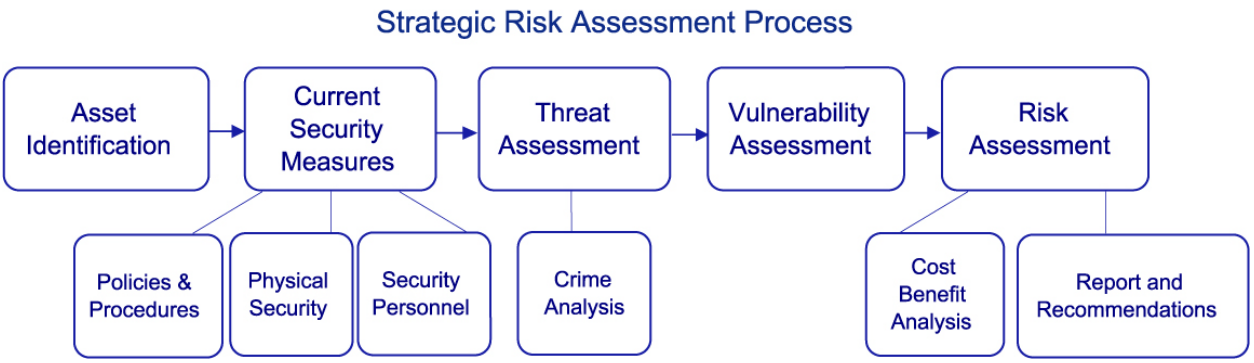

Figure 1 --- Strategic Risk Assessment Process, Copyright ©2006 by Threat Analysis Group, LLC. Used by permission. Additional information available via www.threatanalysis.com.

Before entering into a discussion of the five steps, it might be helpful to identify key security terms and definitions used in this article. Among the more commonly used terms are threats, vulnerabilities, and risks. Generally speaking, threats are acts or conditions that can damage, destroy, or take hospital assets. Examples include natural disasters and criminal perpetrators. Vulnerabilities are weaknesses or gaps in a security program that can be exploited by threats to gain unauthorized access to an asset. Vulnerabilities are those things that make the hospital more prone to security

related problems, such as crime, unauthorized access, and damage from natural disasters. Risk is the result of threats and vulnerabilities. Without the potential for a threat and a vulnerability coming together in time and space, risk is undetermined or non-existent. A simplified example may be a small town hospital which has open access to the facility and limited visitor management (vulnerability), but no historical security incidents (threat), thus the risk to the hospital is low.

Risk = Threat + Vulnerability

Figure 2 --- Risk Formula

Asset Identification

Identifying assets, as seen in the flow chart, is the first step of the risk assessment process. Asset identification is the process of determining what people, property and information are critical to the mission of the hospital. People assets may include doctors, nurses, and patients along with other persons such as visitors and support personnel. A hospital's property assets consist of both tangible and intangible items. Tangible assets are usually simple to identify, while intangible assets, such as the hospital's reputation, are more difficult to identify and assign a dollar value. For all hospitals, information assets include medical records. While all assets have value, not all assets are critical to the hospital's mission. Critical assets, then, are those assets necessary for the hospital to carry out its mission of providing healthcare, for without them functions and processes will fail and cause the hospital's mission to fail. The higher the consequence from the loss, damage, or destruction of an asset, the more critical the asset is. Depending on the type of care and treatment provided, a hospital's critical assets invariably include patients, medical professionals, support personnel, medical records, equipment, supplies, and pharmaceuticals. Other critical assets may not be as evident and must be identified during this step of the risk assessment process. One common way of identifying critical assets is to interviews and/or survey the people charged with carrying out the hospital's mission. Questionnaires of department administrators can also help to identify assets. Regardless of the technique used to identify assets, it is crucial to identify all critical assets to ensure that they are considered during the risk assessment.

Security Inventory

The second step of the risk assessment process is the security inventory. Typically, a hospital has already deployed various security measures throughout the facility or campus to resolve past security problems, thus the risk assessment is measuring mitigated risk, in contrast to raw risk. These security measures may include policies and procedures, physical security equipment, security personnel, or some combination of these measures. Security policies and procedures may include a security management plan, an emergency management plan, workplace violence prevention policy, medical records protection procedures, visitor management policies, and bomb

threat procedures. Physical security equipment can include alarm systems, closed circuit television systems, access control systems, perimeter security systems, and lighting. Security personnel include the proprietary security force, contractual security personnel, off-duty law enforcement officers, and other personnel who serve in a protection capacity. Typical physical security measures will depend on the nature of the hospital, however many physical security measures are common across various hospitals. For example, closed circuit television is commonly deployed at most hospitals.

The risk assessment team should identify each component of the security program, what asset(s) it used to protect, and its level of effectiveness. There are two methods for inventorying current security measures, inside-out or outside-in. Using the outside-in approach, the risk assessment team begins at the facility's perimeter and works their way in toward the identified critical assets through each line of defense. The inside-out approach is the opposite with the team starting at each critical asset and working their way out to the perimeter. In addition to these methods, the inventory process should also include reviewing any available security documentation including security plans, policies and procedures, security officer's post orders, and physical protection system documentation.

Threat Assessment

The third step in the risk assessment process is the threat assessment. Threats are specific events or conditions that seek to obtain, damage, or destroy a hospital asset. Historical information is the primary source for a threat assessment; however other threats may emerge without a historical context. For example, an Avian Flu outbreak is a potential emerging threat to hospitals. Regardless of whether hospital security decision makers are dealing with an emerging or existing threat, they should share information regarding criminal incidents, security breaches, and other threats with other hospitals in close proximity. While hospitals sharing information is an informal approach to threat assessments, formal threat assessments are more detailed analyses used to evaluate the likelihood of adverse events, such as terrorism, natural disasters, and crimes that may affect hospital operations. The focal points of threat assessments are assets (targets) and the threats that seek to compromise those targets. Threat assessments also ask who the bad guys are by evaluating each threat on the basis of capability, intent, and impact of an attack.

The most common form of threat assessment is crime analysis. Broadly speaking, crime analysis is the logical examination of crimes which have penetrated preventive measures, including the frequency of specific crimes, each incident's temporal details (time and day), and the risk posed to a property's inhabitants, as well as the application of revised security standards and preventive measures that, if adhered to and monitored, can be the panacea for a given crime dilemma (Applied Crime Analysis, 2001). While the above definition of crime analysis is holistic, it can be dissected into three basic elements:

- The logical examination of crimes which have penetrated preventive measures
- The frequency of specific crimes, each incident's temporal details (time and day), and the risk posed to a property's inhabitants
- As well as the application of revised security standards and preventive measures

Examining crimes perpetrated at the hospital is commonplace in today's healthcare environment, however it is normally limited to internal security data. External data in the form of crime analysis should also be evaluated to develop a complete picture of threats to the hospital. Crime analysis guides security professionals in the right direction by highlighting the types of crimes perpetrated (crime specific analysis), problem areas on the property (spatial analysis), and when they occur (temporal analysis). Using this information, it is much easier to select appropriate countermeasures aimed directly at the problem. In summary, crime analysis seeks to evaluate actual risk at a company facilities and rank facilities by risk level, reduce crime on the property by aiding in the proper allocation of asset protection resources, justify security budgets, continually monitor effectiveness of the security program, and provide evidence of due diligence and reduce liability exposure.

Vulnerability Assessment

Vulnerabilities are weaknesses or gaps in a security program that can be exploited by threats to gain unauthorized access to an asset. Simply stated, vulnerabilities are opportunities. The fourth step of the risk assessment process is the vulnerability assessment, a systematic approach used to assess a hospital's security posture and analyze the effectiveness of the existing security program. Vulnerability assessments measure the security programs effectiveness, compare it against valid security metrics, and provide recommendations to hospital security decision makers for improvements. In essence, the vulnerability assessment assists hospital security decision makers in determining the need for additional security measures, security equipment upgrades, changes in policies and procedures, and manpower needs. The primary tool of a vulnerability assessment is the security survey which identifies and measures the vulnerabilities at the hospital by determining what opportunities exist to attack, obtain, or damage the hospital's assets.

Security surveys are simply questions and checklists that guide 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 the hospital, including geographic characteristics, and physical layout of the facilities. The security survey also evaluates security deployment schedules, operational requirements, security equipment capability, and internal security incidents which have impacted the hospital security. A

typical hospital security survey would include the following items for consideration by the risk assessment team:

General Hospital Information

Organizational Issues
- *General Security*
- *Visitor Management*
- *Security Force*
- *Policies and Procedures*
- *Emergency Management*
- *Human Resources*

Building Security Survey
- *Perimeter Barriers and Controls*
- *Gate Security and Construction*
- *Vehicle Control and Perimeter Entry Point Access*
- *Clear Zones and Signage*
- *Building Exteriors*
- *Access Control*
- *Lock and Key Control*
- *Outdoor Lighting*
- *Closed Circuit Television (CCTV)*
- *Intrusion Alarms*

Patient Safety

Emergency Center

Infant/Patient Abduction Prevention Measures

Medical Supply Storage Facilities

Information Services (IS)

JCAHO Security Sensitive Areas

Cash Handling

Parking Facilities
- *General*
- *Access Control*
- *Personnel*
- *Lighting*
- *Physical Security Measures*
- *Crime Prevention Through Environmental Design (CPTED)*

Office Area Security

Loading Docks

Risk Assessment

The actual risk assessment is the fifth and final step in the process and is basically the logical analysis of the previous steps which included asset identification, security inventory, threat assessment, and vulnerability assessment. While assessing risk is more of an art than a science, the risk assessment should be benchmarked against industry standards and guidelines. The purpose of risk assessment step is to identify risk mitigation strategies which can be employed to reduce the hospital's risk to an acceptable and manageable level. Mitigating risk involves identifying strategies that can reduce threats and vulnerabilities through the implementation of additional security measures or other means.

Given a specific threat, there are five risk mitigation strategies available to the hospital security decision maker. Generally, the five strategies for managing risk include avoidance, reduction, spreading, transfer, and acceptance. Risk avoidance requires the removal of the target (asset) from the equation. Avoidance is an extreme measure since it can hamper the hospital's operations. Reducing risk involves the deployment of security measures to reduce risk to an acceptable level. Risk reduction is the driving force for a hospital's security department whose role it is to provide protection for assets. Risk spreading is a strategy to move assets to different geographic areas so if one area is attacked; the consequence is limited to that area. Storing necessary pharmaceuticals and other medical supplies off site is good way to spread the risk, thus if an area of a hospital is attacked or damaged by natural disasters, there is another supply available elsewhere. Risk transfer is a strategy used to remove the risk from the owner to a third party. Insurance is the best example of risk transfer whereby the insurance company assumes the risk for a fee. Risk acceptance is another strategy for mitigating risk. As the name implies, risk acceptance is simply where the hospital assumes the risk to an asset, typically after reducing the risk level to an acceptable level.

In summary, assessing risk is a dynamic process that involves continuous evaluation of assets, threats, and vulnerabilities. Reducing the risk to the hospital is accomplished by decreasing the threat level, blocking vulnerabilities and opportunities through enhanced security, or reducing the consequences if a security event should occur. Without question, the best strategy for mitigating risk is a combination of all three elements, decreasing threats, blocking opportunities and reducing consequences. Remember, no hospital is without risk and some risks can be acceptable. Security is a carefully orchestrated balancing act that ensures an open, functional environment of care that effectively protects assets.

Karim H. Vellani, CPP, CSC is the President of Threat Analysis Group, LLC, an independent security consulting firm and is a member of the International Association for Healthcare Security & Safety. He is Board Certified in Security Management and a Certified Independent Security Consultant. As a security consultant, Karim has extensive experience in risk and security management in the healthcare industry. He has 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.

Copyright © Karim H. Vellani. All Rights Reserved.