Hospital Threat Assessments
by Karim H. Vellani, CPP, CSC

In <u>A Study in Scarlet</u>, Sherlock Holmes proclaimed, "There is a strong family resemblance about misdeeds, and if you have all the details of a thousand at your finger ends, it is odd if you can't unravel the thousand and first." That declaration is as true today as it was when Sir Arthur Conan Doyle first wrote it 120 years ago. In essence, Holmes was describing a threat assessment which could tell us that the key to understanding and preventing crime is to dig deeper into each crime incident to determine how it happened. In other words, what vulnerability or weakness in our security program was exploited and contributed to the crime occurrence.

A threat, then, is anything that can exploit vulnerabilities or weaknesses in the hospital's security program. Both actual threats and conceptual threats need to be considered to design a program that protects hospital assets. Actual threats are those that have some historical basis such as infant abductions, patient robberies in the parking lot. Conceptual threats, on the other hand, are crimes or security breaches which may have occurred in only limited frequency at other hospitals or not at all. Certainly, the best example of a conceptual threat on a national level is terrorists using planes as guided missiles before September 11, 2001. A good threat assessment will analyze both conceptual and actual threats. Identifying conceptual threats requires an active imagination and a broad based understanding of crimes that negatively impact other hospitals including those in other geographic areas. Often, threats which are common in other industries or facilities can adapt for attack at hospitals. Thus, a vast knowledge of the many ways in which crimes and security breaches are perpetrated is critical to a robust hospital threat assessment.

Historical information is a primary source for threat assessments, including past criminal and terrorist events. Crime analysis is a quantitative example of a threat assessment, while a threat assessment of terrorism or pandemics is normally qualitative. In the hospital environment, there are a number of common threats, inherent threats so to speak, that are common to all hospitals. These inherent threats include internal and external theft of medical equipment and supplies, patient abduction, and assaults in the Emergency Room. If hospital security personnel know that theft is an inherent threat, why should they perform a threat assessment? We know that theft is a central issue for a hospital's bottom line, but what about other crimes that affect profits in a less obvious way. Violent crime, for example, is a rare crime but the impact is high to both patients and medical staff. If a number of patients are victimized, a reputation for poor security can develop and impact the bottom line. Liability exposure for third-party crimes is also a threat, especially when security levels are not commensurate with the threat.

On the other end of the spectrum is the hospital security professional who engages in *security overkill*, whereby security measures are over-deployed given the threat level, or *security otherkill*, where security resources are directed at a non-existent problem. For example, a hospital experiences a high level of robberies in a short time span decides

to deploy security personnel. The security officers are charged with patrolling the hospital four times per hour, making frequent stops on patient care areas. Despite the increase in security, the robberies persist. What happened? After a thorough analysis of the crime data, the hospital security personnel might find that the robberies were mostly of patient's families in the parking lot. *Otherkill.*

What about the hospital security professional who deploys security based on department heads or doctors who scream loudest. Oftentimes, this leads to security overkill, where departments or other areas of the hospital with a low threat level are afforded a high level of security and areas with high threat levels are provided with minimum security. *Overkill.*

Data Driven Security

It has been argued that the security is more of an art than a science. While that belief is generally true, the business of security is not an art. The security department is a business unit, not unlike other business units within a company that must justify their existence. The higher security moves up the ladder, the more challenges the security director will face and the more business acumen will be required. A commonly accepted business paradigm is *what cannot be measured cannot be managed.* Data driven security refers to using measurable factors to drive a hospital security program and one of the tools for allowing data to drive a security program is a threat assessment. Too often recommendations from the security department are presented with little or no thought to why certain procedures or security equipment should be used. Often, the reason for deploying a security measure is because other companies are doing it. It is all too common in the security industry for there to be a propensity for using certain security measures without complete understanding of the problem or a thorough analysis of the security measures ability to be effective given the specific situation. Threat assessments can help hospital security managers overcome this problem by identifying key concerns. How can security professionals justify to hospital administrators a sizable and usually growing annual security budget? By now, most security managers are keenly aware that a security program's success depends on the commitment and support of hospital administrators. Using anecdotal evidence to justify spending on physical security measures and costly protection personnel no longer suffices. A data driven security program helps hospital administrators understand that security is more than a must-have expense, it justifies costs by showing the proof of success that, when presented effectively, can garner the necessary buy-in from administrators and demonstrate a convincing return on investment. Security expenditures, just like other departmental budgets, need to be justified with empirical data and supplemented with cost-benefit analyses and comparisons.

Security Metrics

Threat assessments are also helpful in developing security metrics which communicate vital information about threats to the hospital and drive decision making. Metrics for various security components, such as the protection force or access control system, can be an effective tool for security professionals to understand the effectiveness of the overall security program. Metrics, as previously discussed, may also identify risk based on failures or successes of security components, and can provide solutions to difficult security problems such as managing a high level of visitors at all hours of the day. Security metrics focus on the results of security decisions such as reduction in thefts after implementation of a Closed Circuit Television (CCTV) or decrease in unauthorized access after deployment of a visitor management system. Security metrics help define how secure we are and assist hospital security professionals in answering basic questions posed by management, such as:

• Are hospital assets protected?

• Which assets need more protection?

• Can the asset protection program be improved?

• What resources should be allocated to security?

• How does our hospital compare to others?

• Are we reducing our liability exposure?

Baseline measurements are often difficult to obtain, especially in the business of security where hospitals are, out of necessity, secretive about their protection systems. In recent years, security industry associations such as ASIS-International, National Fire Protection Association (NFPA), and the International Association for Professional Security Consultants have promulgated guidelines and best practices. In addition to published and accepted industry standards, some courts and state legislatures have outlined baselines of measurement for the security industry. The professional security practitioner will stay abreast of industry standards and the law. While laws must normally be reasonably followed, security professionals may fine-tune published industry standards to meet the needs of their hospitals.

Threat Assessments

As discussed previously, threat assessments are evaluations of human actions or natural events that can adversely affect hospital operations and specific assets. Historical information is a primary source for threat assessments, including past criminal events, while real time information is also being used with increasing frequency due to its availability in some arenas. Threat assessments are used to evaluate the likelihood of adverse events, such as robberies of patients or nurses, against a given asset.

Threat assessments can be quantitative or qualitative. Crime analysis is a quantitative example of a threat assessment. Hospital security professionals use threat assessments as a decision making tool that helps to establish and prioritize safety and security program requirements, planning, and resource allocation.

Threat Information Sources

Hospital security professionals should seek out all possible sources of threat information. Depending on the nature of the assets in need of protection, the sources of threat information may include internal information, security breach investigative reports, law enforcement data, security consultants, media news reports, and industry associations, such as the International Association for Healthcare Security and Safety (IAHSS). Among the basic questions that hospital security professionals should seek answers are:

- What assets have been targeted in the past?
- When were assets attacked?
- Who targeted the assets?
- Why is that asset(s) targeted?
- How was the asset attacked?
- Were any remedial security measures implemented in response to the attack?
- If so, were they effective?

Many hospitals also maintain internal records of security incidents, breaches, and crimes. This information should be reviewed by hospital security professionals on a regular basis while looking for trends and patterns that might indicate existing threats or point to a vulnerability that can be solved with remedial measures. External threat information should also be reviewed. This includes crime data from the local law enforcement where the hospital is located.

Security Reports

A valuable and highly encouraged source of data is in-house security reports. As the name implies, these are reports of criminal activity and other incidents (parking, loitering, and security breaches) which may be of concern to hospital security professionals. These reports may be generated by management directly or through contracted or proprietary security officers. The validity of security reports is only as good as the policy which outlines the reporting and recording procedures, the quality of supervision over security personnel, and the verification process used to eliminate subjectivity. Regardless of the quality of their SRs, management should be cautious not to exclude other sources of data and rely solely on in-house security reports. In requiring the collection of security reports, security managers can stipulate precisely what information is beneficial for their purposes and is contained within each report.

Having said that, security managers should strive to include the following minimum elements:

1. Incident reported
2. Date of incident
3. Time of incident
4. Precise location where the incident occurred on property.
5. Victim(s), if any
6. Witness(es), if any
7. Modus Operandi (MO), or Method of Operation used by perpetrator, if any
8. Follow up investigation(s)
9. Remedy

Law Enforcement Data

Police Data is the most widely used source data for crime analysis because it presents an accurate crime history for a property and is from objective source. Since police departments don't have a stake in a company or any associated liability exposure, their crime data is considered reliable and unbiased. Though some instances of crime statistics manipulation have occurred historically, rarely if ever are the statistics for specific facilities skewed. Most crime data manipulation occurs to overall city crime levels to serve various political goals. At the facility level, there is little reason for law enforcement agencies to skew the statistics.

Another advantage of police crime data is its vast availability due to extensive reporting, capturing, and maintenance of the crime statistics across most jurisdictions in the United States. While costs for the data vary from jurisdiction to jurisdiction, most fees are reasonable. The only downside to police data is the time required to obtain it from police agencies with the necessary time ranging from hours to weeks.

Various crime data and analysis methodologies have been published and used by many cutting edge organizations in the protection of assets. Crime analysis methodologies have been published and subjected to peer-review in various security and police text books, the definitive security book being Applied Crime Analysis.

Law enforcement data is almost always accepted by the courts, and in fact is sometimes required by the courts in determining foreseeability of crime. Though a particular methodology may be subjected to scrutiny, the data is normally admissible. The security professional tasked with testifying on behalf of his organization is safe to rely on crime data from police departments so long as the methodology used is sound.

Assessing Threats

After collecting, reviewing, and summarizing threat information from all available resources, hospital security professionals must apply the threat to specific assets. Critical assets are the primary concern during the assessment, however other assets may also be considered during the assessment phase. The goal of the assessment then is to estimate, quantitatively or qualitatively, the likelihood of occurrence that a threat will attack an asset.

Because of a lack of quantitative data, scenario-driven, qualitative conceptual assessments are appropriate for high value assets that have suffered no prior attacks. A qualitative threat assessment is defined as a type of assessment which is driven primarily by the threats characteristics and are highly dependent upon the assessment team's skills. The threat assessment team or individual, using a qualitative approach, considers each asset in light of the given threat information for that asset, and develops scenarios that may be used by adversaries to estimate the likelihood of attack. Using a qualitative rating system, the threat assessment team assigns a linguistic value to each scenario.

Threat Dynamics

Everyday crimes, rather than terrorism or natural disasters, are the most common threat facing hospital security professionals in protecting their assets and a thorough assessment of the specific nature of crime and security breaches can reveal possible weaknesses in the hospital's current security posture and provide a guide to effective solutions. A full understanding of everyday crime's dynamic nature allows hospital security professionals to select and implement appropriate countermeasures to reduce the opportunity for these incidents to occur in the future. Threat dynamics identifies key elements of each threat and the methods to block specific threats. There are a number of threat dimensions that the hospital security professionals should be well versed in before selecting countermeasures. As conceptually outlined previously, these dimensions include:

• The hospital's situational elements

• Criminal motivation and capability

• The criminal's target selection factors

• Opportunity reduction strategies

Situational elements are those characteristics of the hospital that create an environment which is more or less conducive to certain types of crimes or security violations. For example, a hospital may suffer more from auto thefts in the parking lot than the average number in the community due to the number of targets (patient and staff automobiles) in a small area. Another example of situational elements affecting crime may be the

6

proximity of the hospital to escape routes such as dense fields or wooded areas that can be used to conceal the offender on foot or quick escapes via highways used by the criminal in a motor vehicle. Situational elements also include the nature of the activities that occur on the property. A pediatric hospital, for example, may be more prone to infant abduction.

Criminal motivation and capability is key to understanding the nature of crime on the property. Criminals, more often than not, are rational decision makers capable of being deterred or enticed to commit their acts. In modern criminal justice, it is widely accepted that certain people can be generally deterred from committing crimes given swift and severe punishment. Specific deterrence measures can be taken by introducing countermeasures that increase the risk of detection. For example, the presence of a visitor management system or closed circuit camera systems (CCTV) may deter many criminals. By the same token, people may also be encouraged to commit crime by providing them with ample opportunity and a low risk of detection.

A criminal's ability to select specific targets is a process by which the rational criminal will select the easiest target that provides the highest reward. Criminals also select targets where the rewards are high. Hospital parking lots, for example, provide ample auto theft opportunities for the perpetrator who specializes in stealing cars. One may think of target selection primarily as a force of opportunity. The goal, then, for hospital security professionals is to reduce the available crime opportunities at the facility.

Opportunity reduction strategies address the characteristics of the hospital that either encourage or deter crime. Each hospital will be different in terms of the solutions that are effective because each hospital has its own unique characteristics and unique threats. Unfortunately, what works at one hospital may not work at a similar hospital in a different geographic area. Opportunity reduction strategies may take the form of enhanced policies and procedures, physical security measures, or security personnel.

Accurate threat assessments are critical for hospital security professionals, however, not even the best threat assessment can anticipate every possible scenario including the addition of more assets. Criminals always adapt to and overcome updated countermeasures, and thus, conceptual threats must be identified. In today's world of technology, state of the art countermeasures are outdated at an increasing pace and criminals usually move at a similar pace. Hospital security professionals should keep abreast of the latest threat information using the best available sources of information. Using the threat information sources discussed above and adding to them where possible will assist in keeping the security professional abreast of the latest threats and the assessment report up to date.

Crime happens. As security professionals, we know this to be an undisputed fact and we consider crime when determining the security needs for facilities under our care. More often than not, however, threat assessments are based solely on internal security reports or our memory of security breaches. While this process may be sufficient, a

more robust analysis of threats, as described in this article, can help to further reduce risks to hospital assets and maximize security dollars.

ABOUT THE AUTHOR

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.