Chapter 5

Vulnerability Assessments

In this chapter . . .

- Definition
- Vulnerability Assessments
- Scope of Vulnerability Assessments
- The Vulnerability Assessment Team
- Asset-Based and Scenario-Based Vulnerability Assessments
- Vulnerability Assessment Steps
- Vulnerability Rating Scale
- The Security Survey Report
- The Vulnerability Assessment Report

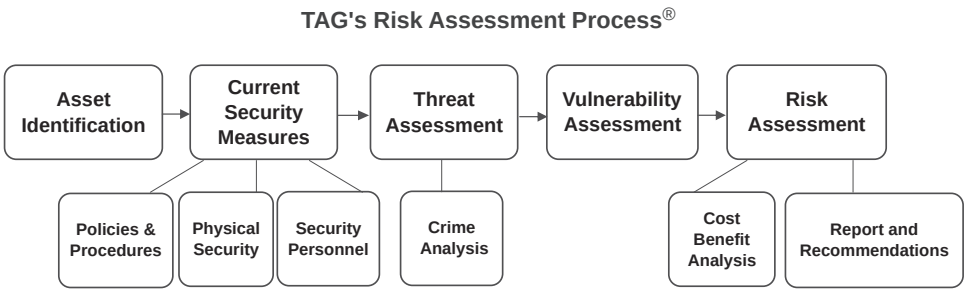

Figure 5-1.
Strategic Risk Assessment Process, Copyright ©2007 by Threat Analysis Group, LLC. Used by permission. Additional information available from Threat Analysis Group, LLC via www.threatanalysis.com.

DEFINITION

In simple terms, vulnerabilities are opportunities. More precisely, they are weaknesses or gaps 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 that provide opportunities to attack assets. Vulnerabilities can be categorized as physical, technical, or operational. Physical vulnerabilities may include structural characteristics of the facility, accessibility by outsiders, geographic location of facility and location of assets within the facility, strength of access control measures, and illumination levels. Technical vulnerabilities may include equipment properties, network weaknesses, susceptibility to eavesdropping and other electronic surveillance, effectiveness of locks, and type and number of cameras. Operational vulnerabilities may include policies, procedures, practices, and personnel actions and behavior.

A vulnerability assessment, sometimes referred to as a security vulnerability assessment, is an analysis of security weaknesses and opportunities for adversarial exploitation in one or more of the preceding categories. The fundamental method for assessing vulnerabilities is the security survey, which is a tool for collecting information about the facility. The goal of a vulnerability assessment is to identify and block opportunities for attacks against assets. By effectively blocking opportunities, security decision makers can mitigate threats and reduce risk.

VULNERABILITY ASSESSMENTS

A vulnerability assessment is a systematic approach used to assess a facility's security posture and analyze the effectiveness of the existing security program at the facility. 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 security decision makers in determining the need for additional security measures, security equipment upgrades, changes in policies and procedures, and manpower needs.

Vulnerability assessments identify security weaknesses that can be exploited by an adversary to gain access to the organization's assets. For example, a vulnerability assessment may reveal gaps in security in an investment bank's financial management system; security weaknesses that limit the ability of a nursing home to protect its residents; or security gaps in a national monument's visitor management process. The goal of vulnerability assessments is to ensure life safety, protect assets, and promote continuity of operations. The driving forces

behind vulnerability assessments include new legislation, revised threat assessments with new or emerging threats, increased criticality of assets, concern for continuity of operations, and newly recognized vulnerabilities. A comprehensive vulnerability assessment affords security decision makers and facility management personnel the opportunity to make future planning decisions based on an acceptable methodology that can be used for budget considerations, capital expenditures, personnel allocation, and procedural guidelines.

The vulnerability of an asset is determined by the potential weaknesses in operational processes and procedures, physical security weaknesses, and technical gaps that can be exploited to attack an asset. Vulnerability assessments are used to identify these weaknesses by way of a security survey. To paraphrase noted author Charles A. Sennewald, 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 an organization's existing operation and facility. The purpose of a security survey is to measure the vulnerabilities at a facility or of specific assets by determining what opportunities exist to exploit current security policies and procedures, physical security equipment, and security personnel. The outcome of a security survey is a report, normally written, that outlines a series of solutions that, if implemented, will reduce the short-term and long-term opportunities at a facility. Security surveys are designed to meet the unique needs of a facility or type of facility. For example, one may use a security survey designed for a maritime port facility for other port facilities, but a maritime port facility security survey will not likely meet the needs of an office building. Even within similar-type facilities, unique characteristics must be considered and included in the security survey.

Security surveys are simply questions and checklists that the assessment team must complete 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 facility, physical layout of the facility and its unique characteristics, security and other personnel, operational requirements, security equipment capability and deployment schedules, and threats and other incidents that impact security. General information normally captured in a security survey includes:

- Vulnerability Assessment Team (identify by name and title)
- Date
- Name of Facility/Site
- Emergency Contacts and Telephone Numbers
- Law Enforcement Jurisdiction (agency name, address, and phone number)
- Main Facility Telephone Numbers
- Site Address

- Site Description
- General Purpose of Site
- Open to Public
- Normal Operating Hours
- High Activity Use (hours/days)
- Other Tenants or Users of the Site
- Individuals Who Have Access to Critical Areas
- Location of Critical Assets within the Facility
- Known Vulnerabilities

Scope of Vulnerability Assessments

The scope of a vulnerability assessment depends on the goal of the security team. Some assessments are geared toward protecting only the most critical assets, such as an assessment that emphasizes only the reduction of violent crime opportunities to protect people at the facility. Other vulnerability assessments emphasize the full range of opportunity-reduction strategies for all critical assets and lesser assets.

One may wonder why there is a difference in scope among vulnerability assessments. Normally, a truncated scope is in reaction to a particular threat or the identification of a new critical asset. Sometimes, a limited scope vulnerability assessment is the result of a need coupled with finite resources, typically time and money. Independent security consultants face this often where management identifies a need for a vulnerability assessment based on a new threat and has limited funds in which to execute the assessment. The threat assessment, for example, which is normally conducted prior to the vulnerability assessment, may have identified and prioritized threats, and these high-ranking threats serve as the scope of the vulnerability assessment. Simply prioritizing threats will lead to a limited scope assessment. For example, a hospital that operates one main facility and several medical clinics off campus may decide to pursue the primary, most attractive target first and leave the other facilities for another budget cycle.

Regardless of the range of the scope, the assessment team often uses a written mission statement to guide the vulnerability assessment. This statement identifies the stakeholders and outlines the assessment's objectives. The stakeholders include the company that owns the facility, the organization's employees, the people who frequent the facility, possibly the community at large, and possibly all of society. The mission statement identifies the key issues that are of interest to the stakeholders. A sample mission statement for a hospital vulnerability assessment may be: *To perform a vulnerability assessment that identifies security vulnerabilities, opportunities for security breaches, and hazards on the hospital's premises that can adversely affect the employees, visitors, and patients of the hospital.*

Key to the vulnerability assessment is project management. The vulnerability assessment team leader is best suited to take on the role of project manager. Project management includes defining the scope of the assessment, refining the security survey for the unique needs of the facility, and determining a project work plan, time line, and milestones. The project manager should also define the role of each assessment team member and arrange for all resources needed for the assessment, such as light meters, facility access, and measuring tape.

The Vulnerability Assessment Team

An important quality for the vulnerability assessment team is the ability to think like an adversary. When conducting the assessment, the assessment team should consider three focal points: how an adversary can carry out a specific type of attack against a specific asset or group of assets; how effective existing security measures are in deterring, detecting, and delaying the specific attack; and the current level of vulnerability. This last item should have either a quantitative or qualitative value assigned. The attack modes considered will have been developed during the threat assessment and are used in conjunction with targeted asset lists to assess vulnerabilities based on predetermined performance metrics or against accepted security guidelines.

The assessment team should include not only security personnel, but also personnel intimately familiar with the facility under assessment and specialists as needed by the facility. The project manager should be familiar with various assessment methodologies unless a particular methodology must be followed. For example, Sandia National Laboratories Risk Assessment Methodology for Water Systems (RAM-W) may be required by the facility. The team should also include experts or specialists as needed. Blast analysis specialists and structural engineers, for example, may be needed for a water system or dam. Of primary consideration to be included on the team are people with precise knowledge of the processes and procedures that occur on the facility as they relate to critical assets.

Depending on the nature of the vulnerability assessment, a team may consist of as few as one person or its size may range much higher. Typically, the assessment team is made up of three to eight people. On smaller teams, the project manager's role is often shared by a general security management person, while other roles may include a technical security professional and a person familiar with the facility. Often, the assessment team includes external personnel such as consultants experienced in conducting assessments for various types of facilities and exposed to other security systems. One of the greatest advantages of an outside consulting firm is the range of security strategies they bring to the current vulnerability assessment. Having had experience in different and similar facilities and through the process of trial and error, security consultants usually have more experience than internal personnel in conducting vulnerability assessments.

ASSET-BASED AND SCENARIO-BASED VULNERABILITY ASSESSMENTS

Vulnerability assessments tie assets to threats in an effort to identify potential vulnerabilities and countermeasures to reduce those vulnerabilities. The level of vulnerability of each asset and threat is evaluated using either an asset-based or a scenario-based assessment.

Asset-based vulnerability assessments are broad evaluations of assets and the threats that impact those assets. For example, an asset-based assessment at a jewelry store will focus on the jewelry as the primary asset in need of protection and the threats that may impact on the jewelry. Asset-based assessments assume that every scenario cannot be imagined or that those that are imaginable are too speculative to consider.

Scenario-based vulnerability assessments, on the other hand, focus on the attacks themselves. The scenario-based assessment evaluates vulnerability by asking how targets might be attacked. This type of assessment requires knowledgeable assessment team members who have an understanding of history and can foresee the methods used by adversaries in the future. While history is a primary indicator, not all future threats can be anticipated based on past attack modes. Certainly, the September 11 attacks are evidence of a new attack mode that was not anticipated, at least not by the masses, prior to 2001. Scenario-based assessments are advantageous in that they are better suited for assessing high-value assets and high-consequence attacks. Unfortunately, this advantage also creates a problem whereby lesser threats are ignored and security measures are not implemented. The scenario-based vulnerability assessment process includes the following six steps undertaken by the vulnerability assessment team:

1. Selects the scenario to evaluate.
2. Studies the target's (asset) characteristics.
3. Evaluates certain types of adversaries and attack modes.
4. Evaluates the likelihood of the existing security measure's ability to deter, detect, or delay the attack.
5. Analyzes the consequences of the assets loss, damage, or destruction.
6. Assigns a vulnerability rating.

The attack scenarios are normally selected by the vulnerability assessment team from the high-consequence alternatives. While the team's goal is to be creative, the scenario must be sufficiently realistic. A fair assessment of the target's attractiveness, from the adversary's perspective, is critical to accurately evaluate the strengths and weaknesses of each asset. Although it is easy to theorize about well-trained, skilled, and properly equipped adversaries, the team should not create an infallible threat. History has shown repeatedly that adversaries

make mistakes. The next step is to evaluate the likelihood that the existing security measure will deter, detect, or delay the attack. Typically, an outside-in approach is used whereby the assessment team identifies the outermost layer of protection and works its way inside toward the assets, passing through each protection layer in the same order in which an adversary would go. 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 loss, damage, or destruction of the assets and assigns a vulnerability rating.

An example of a scenario-based vulnerability assessment is one where the assessment team selects a low-grade explosion outside a government building as an attack scenario. They postulate that the explosion occurs immediately outside the building during normal business hours. What are the characteristics of the building and its assets (employees and other people would be among the critical assets) 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, there is a downside to scenario-based assessments, in that these types of assessments force the team to focus on protecting against particular threats and possibly ignoring other threats. Nevertheless, both asset-based and scenario-based vulnerability assessments will result in a list of recommendations for changes to the security program.

Vulnerability Assessment Steps

Like threat assessments, vulnerability assessments may be quantitative or qualitative depending on the nature of the assessment and the availability of metrics. In both scenario-based and asset-based vulnerability assessments, the general steps are as follows.

1. Identify assets in need of protection.
2. Review historical security and incident information if available.
3. Prepare a security survey.
4. Identify existing security measures for each asset and determine the effectiveness of each measure individually or in combination with one another.
5. Assign a rating to each asset based on a quantitative or qualitative vulnerability rating scale.
6. Prepare a written report with recommendations for additional security measures or changes to the security program.

Step 1 assumes that the vulnerability assessment is not being conducted as part of an overall risk assessment and therefore assets have not yet been identified. If the vulnerability assessment is being conducted as part of a risk assessment, then the asset information should be readily available to the assessment team.

Step 2 also assumes that the vulnerability assessment is not being conducted as part of an overall risk assessment and therefore a threat assessment has not yet been conducted. If the threat assessment is already completed, reviewing the threat assessment report should indicate any vulnerabilities that adversaries have exploited in the past. For example, the threat assessment report indicates that security personnel have responded to an alarm generated from camera 7 repeatedly during the past year. The vulnerability assessment team determines that camera 7 surveys the right rear perimeter fencing of the facility. Upon inspection, the assessment team finds that the fencing in that area is in disrepair and is an older design relative to the fencing in the front of the facility.

Step 3 of the vulnerability assessment is to prepare the security survey. There are many sources of security surveys, limited only by the assessment team's creativity. Previous vulnerability assessments may also be refined, updated, and used for the current assessment. Numerous security books contain sample security surveys and various industry organizations that have developed surveys specific to their industry.

Step 4 of the vulnerability assessment is to identify existing security measures for each asset and determine the effectiveness of each measure individually or in combination with one another. As the team assesses the facility, existing security measures designed to address known security gaps are identified and noted on site diagrams or blueprints. Depending on the nature of the facility and the type of security measures in place, the countermeasures may be tested and compared to established metrics and industry standards. One of the biggest mistakes a vulnerability assessment team makes is to assume that existing countermeasures are adequate and to counter the threat. Using performance testing, the team can determine whether the countermeasures are doing what they were designed to do, that is, reduce the vulnerabilities. Experienced assessment teams will analyze the facility from the adversary's point of view rather than from the security decision maker's perspective. What factors may deter the motivated offender? What paths might the attacker take into the facility? What tools will be required to defeat security measures? Will stealth or deceit be necessary? Will an insider be needed? Technical security people are also beneficial to the overall evaluation of existing security measures in that they will know the limitations of electronic measures. The vulnerability assessment team conducting an asset-based assessment will spend more time in the field assessing routes to assets, identifying points of detections, and determining lines of defense. The scenario-based assessment team will spend more time brainstorming and conducting table-top exercises in an effort to assess worst case attacks and consequences to the facility's most critical assets.

Step 5 requires that the vulnerability assessment team assign a vulnerability rating to each asset based on a quantitative or qualitative vulnerability rating scale. These scales are discussed in detail at the end of this chapter. For now, it is important to understand that each vulnerability is rated based on the assets value (qualitative or quantitative), the threat posed, and the security measure's effectiveness in reducing the opportunity for vulnerability exploitation. The rating will also be dependent on the consequence of loss, damage, or destruction. For manufacturing-type facilities, this is measured in operational downtime and loss of revenue, both of which can be measured quantitatively.

In step 6, the vulnerability assessment team prepares a written report summarizing the assessment and recommendations for additional security measures or changes to the security program to reduce the overall vulnerability level and the vulnerability level of specific assets. The report should also include a basic cost-benefit analysis outlining the reduced vulnerability level that may be achieved after implementing recommended security measures. Some of the factors the assessment team should consider in their report, especially for critical facilities, are

- Facility population
- Structural integrity of facilities
- Land area of facility
- Distance to emergency services
- Redundant power supply
- Closed circuit television (CCTV) systems
- Intrusion detection systems
- Barriers
- External lighting
- Armed security personnel

Vulnerability Rating Scale

Vulnerability ratings are based on the attractiveness of the target and the level of protection afforded those assets. The rating scale can be either quantitative or qualitative. Qualitative ratings are scaled by relative value to the organization's mission. Quantitative ratings are based on life-cycle costs, including the actual value of the asset, replacement cost, operational costs, maintenance costs, and costs associated with time lost while the asset is replaced or repaired. A simple example will illustrate the point. If your personal car were to be stolen, the current value would be lost, plus the cost of purchasing a new car, plus the cost of transportation between the car's loss and replacement.

Qualitative Vulnerability Rating Scale

An example of a qualitative vulnerability rating scale for facilities is as follows:

Very High—A facility with attractive targets, a history of threats, inadequate security measures, and adversaries capable of exploiting the security weaknesses. An attack on this type of facility may include structural damage, operations may be severely hampered or completely stopped, and assets contained within the facility may be destroyed.

High—A facility with attractive targets, no history of threats, inadequate security measures, and adversaries capable of exploiting the security weaknesses. An attack on this type of facility may include some structural damage, operations may be reduced to only the most critical, and assets contained within the facility may be destroyed.

Moderate—A facility with attractive targets, no history of threats, adequate security measures, and no adversaries capable of exploiting the security weaknesses. An attack on this type of facility may affect normal operations with minimal downtime.

Low—A facility with no attractive targets, no history of threats, and adequate security measures. An attack on this type of facility will cause minimal disruption to normal operations.

Security Survey Areas for Hospitals

General 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)
Joint Commission on Accreditation of Healthcare Organizations Security Sensitive Areas
Central Plant
Cash Handling
Parking Facilities
- *General*
- *Access Control*
- *Personnel*
- *Lighting*
- *Physical Security Measures*
- *Crime Prevention Through Environmental Design (CPTED)*

Office Area Security
Loading Docks

The Security Survey Report

The security survey report is the result of an on-site review of the facility or an asset's vulnerabilities and security measures. While the typical security survey report does not comprehensively address all facets of the vulnerability assessment, it does address the vulnerabilities and security measures, and provides recommendations. A typical security survey report includes general information about the facility, a review of critical assets, some form of threat assessment, an outline of existing security measures, a description of vulnerabilities, and recommendations for security changes. Noticeably absent from the preceding security survey report sections are the cost-benefit analysis and vulnerability ratings, which are not normally included in the security survey report.

Depending on the scope of work, security consultants often use a letter format for their security survey reports. According to Sennewald and Vellani in *Consultants as a Protection Resource*, Protection of Assets Manual, 2004, "The scope of [the consultant's] work refers to the central objective of the consulting task, or the clear focus of the effort." A very limited scope consultant's report is presented in Figure 5-3 and a large-scale risk assessment report is presented in the next chapter. The report in Figure 5-2 demonstrates a phased approach to vulnerability mitigation wherein certain elements of the security program are modified and new security measures are added. The effects of

these measures are allowed to take place over a fixed period of time, and then the threat and vulnerability level are reassessed before implementing phase 2 recommendations. The time between assessments and deployment of the next phase may be very short or as much as one year.

Report for a Limited Scope Security Survey

October 26, 2002

James Buchanan, Director of Facilities & Safety
Anytown Medical Center
14623 North Freeway
Anytown, PA 15213
Re: **Security Survey**

Dear Mr. Buchanan:

Per your request, I have completed a security survey for Anytown Medical Center (AMC). The report is multi-phasic in that it recommends a number of relatively cost effective steps (Phase 1) that may reduce the opportunity for crime on the property with escalating measures (Phase 2) for persistent issues. Phase 1 issues should be addressed immediately and evaluated in a reasonable time after implementation. Phase 2 measures may be implemented in whole or in part as needed after evaluation of the effectiveness of Phase 1 measures.

This report is based on the following:

1. Crime and Foreseeability Analysis (January 1, 2000 to December 31, 2002)
2. Meetings with management and security personnel to gather facts regarding the property
3. Day and night exterior security inspections
4. Parking Lot Lighting Survey
5. Crime Prevention Through Environmental Design (CPTED) analysis

I have also reviewed the following documents relevant to this security survey:

1. Security Management Plan
2. JCAHO Standards
3. Site Diagrams
4. AMC Security Incident Reporting for 2000, 2001, and 2002
5. AMC Security Department. Policies and Procedures
6. Anytown Police Department (APD) crime records pertaining to 14623 North Freeway (January 1, 2000 through December 31, 2002)

General Information

AMC is located in a hybrid commercial/residential area with low traffic on surrounding streets and high traffic along the main entrance adjacent to Interstate 10. There is an internal security manager and a facility manager responsible for security of the facility. Additionally, there are two unarmed (noncommissioned) security officers on duty 24 hours a day, 7 days per week except during the daytime hours when

the security manager fills the role of one security officer. At times, there is additional security provided by police officers.

Crime Analysis

Internal security incident reporting for 2000, 2001, and 2002 indicates that the most common security issue is theft-related concerns, specifically auto theft, burglary of automobiles, and theft of property.

An external crime analysis was conducted for the property for the dates January 1, 2000 through December 31, 2002. During this period, APD records indicate that no murders occurred on the property. The records also indicate that 12 violent crimes were reported from the address, including 1 rape, 3 robberies, and 12 aggravated assaults, with two of these occurring in 2002. For a detailed listing of crime, please review use the CrimeAnalysis™ software provided as a supplement to this report.

Phase 1: Obtain official crime data (Calls for Service and offense reports) from the police department for the property annually.

Phase 1: Review both internal security incident reporting and external crime records and make any appropriate security changes.

Phase 2: Obtain official crime data (Calls for Service and offense reports) from the police department for the property every six months.

Foreseeability Analysis

No *recent* pattern or trend of *violent* crimes on the property would indicate any foreseeable violent crimes. Offense reports for the two violent crimes that were reported from the premises during 2002 indicate that they occurred on the road.

Phase 1: Implement a system to notify employees and others of violent crimes on the property.

Phase 1: Retain Security Daily Activity Reports (DARs), light check reports, and other security documentation for a period of five to seven years.

Liability Analysis

A security expert will likely attack the following possible security vulnerabilities:

1. No ongoing effort to monitor crime on the property (Crime Analysis attached)
2. Lighting of the property (see "Lighting" below)
3. Location of AMC in a "high-crime area" (subjective)
4. Numerous hiding places due to high shrubs and fencing (see CPTED below)

Crime Prevention Meetings and Security Training

Security training is provided to employees during orientation and annually thereafter.

Phase 1: Continue this training and maintain logs of employees in attendance.

Phase 1: Implement a program to provide training to security officers on an ongoing basis, including daily briefings, CPR, crisis intervention, workplace violence, refresher courses, and understanding of policies and procedures.

Phase 2: Require that security officers undergo International Foundation for Protection Officers training and obtain certification of Certified Protection Officers (CPO) or similar training.

Phase 2: Implement crime prevention meetings on a biannual basis to inform employees of current risks and protection measures, including personal protection.

Internal Crime

Thefts comprise the majority of incidents at the facility, according to both internal security incident reporting and external crime records.

Phase 1: Institute a "Clean Desk Policy" that works toward reducing the opportunity for thefts of employee purses and other personal items.

Crime Prevention Through Environmental Design (CPTED)

CPTED is a security tool that manipulates the environment to reduce opportunities for crime. It includes the concepts of natural access control, natural surveillance, and territorial reinforcement to reduce crime opportunities.

Phase 1: Install benches in the various open areas in front of the hospital for use by patients, employees, and visitors. This will create a sense of territoriality and allow surveillance of the parking areas and hospital entrances.

Phase 1: Permanently seal parking lot entrances, keeping open only those that are necessary for effective traffic movement.

Phase 1: Close unnecessary entrances at night.

Phase 1: Trim back or remove trees to create more common space for patients, employees, and visitors to gather and "claim territory," thereby showing would-be offenders that the area is "under surveillance."

Phase 1: Plant thorny shrubs near blind corners to deter use as a hiding place.

Phase 1: Trim (or replace) shrubs that are not along a fence line to 3 feet.

Phase 2: Install a security "shack" at the front of the main entrance.

Access control

Exterior doors, except the emergency room entrance, are locked at 2000 hours and checked by security officers during their patrols. A checklist is used during the patrols for both interior and exterior doors, ensuring that the doors are secure. Some of the doors are key controlled, while others have card key access.

Phase 2: Install a uniform card key access system that also allows security officers to scan their card while they patrol. This system should allow "writing" to a main database that will allow analysis of who and when a certain card is scanned.

Access is further limited to the property by various fences that form the perimeter of the property. These fences are generally in good repair; however, they are not security height (7 feet) with overhang, and there is no clear zone.

Phase 2: Increase fence height to 7 feet with overhang.

Security Personnel

Two noncommissioned security officers are present on the premises 24 hours per day, 7 days per week. The weekday security force schedule is as follows:

Personnel	Start	End
Security Manager	0800	1600
Security Officer	0700	1500
Security Officer	1500	2300
Security Officer	1600	0000
Security Officer	2300	0700
Security Officer	0000	0800

The weekend shifts are 0800 to 2000 and 2000 to 0800, with two officers on during each shift. The security force is equipped with a golf cart to patrol the grounds and a radio for communications.

Phase 1: Do not, except under special circumstances, provide employee escorts, as it takes the security officer away from his duties.

Phase 1: Provide reasonable supervision over the security officers.

Phase 1: Security personnel should vigilantly inspect and scrutinize visitors, contractors, and other outsiders for possible security breaches.

Phase 1: Ensure that security officers are following post orders.

Phase 1: Replace burned out light bulbs each morning as reported in the security officer's DAR.

Phase 1: Include a program for periodic Quality Control inspections of security personnel.

CCTV

Analog closed circuit television is currently utilized at this facility.

Phase 1: Install monitors in the security office, allowing for security officers and security managers to monitor the currently installed cameras.

Phase 2: Install digital CCTV cameras in strategic locations outside the facility to monitor the parking areas, emergency room areas, and perimeter.

Lighting

The lighting is generally below standard for parking areas. There are many dark areas outside the facility, including shadows that may be used as cover for a criminal.

Phase 1: Include a nightly light check as part of the security officer's patrol.

Phase 1: Replace lights that are inoperable the following day.

Phase 1: Increase lighting to 2.0 fc (foot-candle) in the parking areas.

Phase 1: Increase lighting at entrances.

Policies and Procedures

AMC has a written security management policy.

Phase 1: Monitor that practice follows the written policies and procedures.

Phase 1: Ensure that the policies and procedures are fluid in that they can be revised to meet future needs.

Quality Control/Performance Monitoring

Currently, all supervision is provided by internal management personnel.

Phase 2: AMC should include monthly quality control inspections of security operations by an independent, third-party inspector to validate the effectiveness of the security force.

Should you have any questions or if I can be of further service to AMC, please feel free to call me at (281) 494-1515. Thank you for the opportunity to serve AMC.

Respectfully submitted,

Karim H. Vellani, CPP, CSC
Licensed and Certified Security Consultant

The Vulnerability Assessment Report

The vulnerability assessment report is a critical component of the overall risk assessment and is used to document the assessment activity. While the report may be formatted to fit the needs of the organization under assessment, a typical vulnerability assessment report includes the following sections.

Table of Contents

The table of contents is an often overlooked section of the vulnerability assessment report. Each major report section as well as subsection should be identified with its corresponding page number. A comprehensive table of contents is beneficial because an index is rarely included in a vulnerability assessment report.

Executive Summary

The executive summary is an overview document used to provide a condensed version of the entire report. It is prepared to cover the highlights of the report for those decision makers who do not have the time to read the full report. Executive summaries tell the report's audience what is significant within the report and what issues the decision-making readers must respond to. While covering each section of the full report, the executive summary should not be longer than 10 percent of the full report and are often much shorter and should be a stand-alone document. Generally speaking, the executive summary should cover the scope and objectives of the vulnerability assessment, team composition, vulnerability assessment methodology utilized, facility assessed, date(s) of

assessment, threat assessment information, critical assets assessed, conclusions, and recommendations. The assessment team should take caution with the recommendations within the executive summary since this document does not typically include justifications for each recommendation.

Background

The background section of a vulnerability assessment outlines the scope of the assessment, critical assets, and facility characterization, and provides an overview of the assessment methodology and process. A summary of the threat assessment report is also normally included.

The vulnerability assessment team's first on-site task should be to review the facility characterization resulting from the asset identification and threat assessment risk assessment steps. This is an important step to understand the facility, what assets specifically are in need of protection, and the threats posed to those assets. The facility characterization should include a concise description of the organization's mission, the criticality of the facility under assessment, major functions and processes, and key staff used to ensure that the mission is carried out. Also included in the facility characterization are the geographic location, property boundaries, access points, physical and structural characteristics and condition, and significant features of the facility. Occupant information, traffic patterns, neighboring facilities, and community demographics also should be included. The facility characterization may also address supply chain and transportation information, regulatory and legal requirements that impact the facility, and security policies and procedures in effect. A savvy vulnerability assessment team, especially a team consisting of external personnel, will also seek to understand the organization's mission so as not to trample on it.

The facility characterization will include a review of facility blueprints, site diagrams, and floor plans; identification of property boundaries; location of authorized access points; and maps depicting facility ingress and egress paths. The characterization may also include a description of physical structures, traffic patterns, and neighboring facilities. Reviewing threat information during the facility characterization is advised. This information may come from interviews or from a formal threat assessment report. Internal security records, authorized users lists, and operational logs may also be reviewed. For purposes of understanding operational vulnerabilities, the assessment team should be aware of any differences during different operational shifts at the facility. This includes an awareness of normal activities and functions that occur during each shift as well as traffic levels of employees, contractors, and visitors. Finally, the facility characterization should include a list of critical assets as identified in step 1 (Asset Identification) of the risk assessment process and describe the operational consequences if those assets were to be lost, damaged, or destroyed.

Blueprints, site diagrams, and floor plans should be reviewed during the facility characterization because they may be used to identify property borders, ingress and egress routes to the facility, specific vulnerable areas in and around the facility, adjacent facilities, physical structure locations, and features outside the facility such as railroads, waterways, interstate highways, and airports.

The assessment methodology and process should include the various types of assessments conducted, including operational, structural, and procedural assessments. The operational assessment may outline the types and lengths of work shifts, activities typical to each shift, security implications, and availability of protection forces. The structural assessment methodology should describe how physical structures were assessed. For example, what type of materials make up the roof, walls, windows, floors, and foundation? How are the heating, ventilation, and air conditioning (HVAC), sewage, and water systems secured? A procedural assessment describes the processes and procedures in place at the facility. This includes the access control procedures for employees, contractors, and other visitors such as delivery people and vendors. How are hazardous materials transported into, out of, and inside the facility? How are vehicles inspected while entering and leaving the facility?

Assessment Overview and Process

The assessment overview and process section describes the facility's critical functions, significant threats, and documentation available. The primary goal of this section of the vulnerability assessment report is to detail comprehensively the major vulnerabilities at the facility. Of primary concern is the functionality of the physical protection system.

Typical physical security measures will depend on the nature of the facility. However, many physical security measures are common across various applications. For example, fencing is appropriate at most facilities, even in open campuses such as universities where certain facilities may be fenced. The vulnerability assessment team should identify each component of the physical security system and decide what level of effectiveness is required for the facility and what risks management is willing to accept. Why would the team even consider anything less than maximum effectiveness? No physical security system can maintain maximum effectiveness. Documenting the assumed risks is part of the team's due diligence effort.

The effectiveness level of a physical protection system (PPS) is a factor in its ability to deter potential adversaries, detect those that are not deterred, and delay adversaries until the protection force can respond. Each of these functions should be built into the physical protection system, performed in order, and take less time to activate than it takes for the adversary to reach its intended target. An effective physical protection system provides protection in depth, with multiple layers of security that force the adversary to defeat each layer in

order, minimize the consequences of individual component failure by having redundancy, and exhibit balanced protection no matter which path of attack the adversary chooses.

As discussed earlier, the first function of a physical protection system is to deter the potential adversary. Deterrence is a security strategy designed to discourage adversaries by increasing the risks to the adversary, promoting a sense of security, and instilling doubt on behalf of an adversary. Failing an ability to deter a would-be adversary, the physical protection system should detect the presence of the adversary. Detection is a security strategy designed to assess the threat and alert security personnel of an adversary's presence. Cameras and sensors are examples of detection measures. Once the adversary has been detected, the physical protection system should delay the adversary from meeting its objectives until the protection force can respond to neutralize or defeat the adversary. Delay, then, is a security strategy designed to slow the progression of adversaries into or out of the facility, and defeat is another security strategy designed to neutralize adversaries before an asset is lost, damaged, or destroyed. Barriers are an example of a delay measure. The physical protection system model described applies to most protection situations, from Fort Knox to home defense.

Here again, it is important to note that a common mistake made during the vulnerability assessment is to assume that existing countermeasures are adequate in effectively countering the threat and reducing vulnerabilities. The use of security metrics is helpful in determining whether the system is optimally configured and deployed. Vulnerability of the physical protection system can be both quantitatively and qualitatively measured depending on the nature of the component. False alarm rates (FAR) and nuisance alarm rates (NAR) can be measured quantitatively and compared against industry metrics. Protection force response times can also be measured quantitatively and benchmarked against average response times for different types of threat levels.

The vulnerability assessment team should address each physical protection system area separately beginning with deterrence measures. Among the more common deterrence measures are highly visible, uniformed security personnel, lighting, signage, and other countermeasures such as fencing and natural barriers that may intimidate adversaries and tip the risk-reward balance in favor of security.

Detection measures present in the physical protection system should be addressed next. Detection security measures should be located throughout the facility but primarily at the perimeter to increase the time between detection and the security force's response. These measures include both interior and exterior intrusion detection systems, as well as their individual components such as sensors, closed circuit television systems, and clear zones. Among the questions that the vulnerability assessment team should be asking during the security survey are:

- What is the key control process?
- How are packages screened prior to entry into the facility?
- Are X-ray machines and magnetometers used, or are people and packages screened visually?
- What access control measures are in place to allow entry to only authorized personnel?
- Are there multiple entry points?
- Are vehicles screened when leaving sensitive areas?
- Are perimeter intrusion detection measures such as sensors operating properly?
- Do environmental factors, such as terrain and weather, negatively impact the ability of sensors to detect intrusion?
- Have any past attempts to penetrate the facility's access control systems been successful?
- Is the physical protection system adequately assessing alarms?
- Are the false alarm and nuisance alarm rates at a minimum?
- Are cameras able to adequately detect unauthorized entry at all points around the perimeter?
- Are CCTV systems monitored by security personnel or electronic means?
- Are intrusion detection systems, CCTV, and other electronic measures monitored on- or off-site?
- Are all CCTV components (switching equipment, video monitors, transmission lines) working as designed?
- Are lighting systems fully functional?
- Do lighting systems meet the various codes and standards such as the Illuminating Engineering Society of North America's Guideline for Security Lighting for People, Property, and Public Spaces (IESNA G-1-03)?

The list can go on ad infinitum, but suffice it to say that the security survey items should be comprehensive to meet the facility's needs and the assets in need of protection.

Delay, as we have discussed, is a security strategy designed to slow the progression of adversaries into or out of the facility. Delay comes into play after detection measures have signaled an actual intrusion, effectively blocking out false alarms, and the protection force has been notified. The response team may or may not be located on site. For example, low-security facilities, such as office buildings, may not have a response team on site, but rather may have a team on roving patrol for numerous facilities. Regardless of where the protection

force is located, the delay security measures should slow the progression of the adversary toward its intended target, allowing enough time for the protection force to arrive and neutralize the threat. Delay measures include locks, doors, walls, fences, and barriers. The United States Army has published numerous penetration times relating to different types of delay measures, and depending on the type of facility under assessment, these standards should be consulted.

The protection force is probably the most difficult security measure to address in the vulnerability assessment. Depending on the nature of the facility, there may not be a traditional protection force, but rather designated personnel responsible for responding to distress and alarm signals. The key factor to assess is response times, which is an excellent security metric that the vulnerability assessment team should monitor and evaluate during the vulnerability assessment. On-site personnel responsible for security should also constantly monitor response times to ensure that the protection team is operating at an optimum level. The protection forces should also be evaluated for appropriate equipment and training on any prescribed equipment. Protection force equipment includes communication devices, vehicles, firearms and other weapons, incident reporting mechanisms, personal protection equipment, and so on. The vulnerability assessment team should also evaluate policies and post orders, especially those relating to the use of force. Patrol records and daily activity reports (DARs) can shed light on protection force effectiveness.

Conclusions

The conclusion section of the vulnerability assessment report is used to summarize the vulnerabilities and provide the reader with the vulnerability ratings. The vulnerability ratings may be quantitative, qualitative, or a hybrid depending on the nature of the vulnerability.

Deficiencies should be noted in sufficient detail to provide justification for the recommendations to follow in the next section.

Recommendations

The recommendations section of the vulnerability assessment report includes the assessment team's suggested changes to the security program. These changes may include the deployment and redeployment of security personnel, additional physical security measures, and updates to security plans, policies, and procedures. The recommendations should be prioritized based on the vulnerability ratings for each asset, allowing the security decision makers to move forward with changes in an appropriate fashion. Cost-benefit analysis and cost estimates should also be included in this section of the vulnerability assessment report. Cost-benefit analysis is important since budget requests will have to be made and costs justified. Recommendations may also be made in phase with threats, and vulnerabilities should be reaassessed between phases.

Appendices

Appendices may be included in the vulnerability assessment report and usually contain facility and area photographs, blueprints, site diagrams, and floor plans. It is also helpful to the reader to include a copy of the security survey checklist and any cost-benefit analysis documentation.

Vulnerability Assessment Report Outline

I. Table of Contents
II. Executive Summary
    A. Vulnerability assessment dates
    B. Scope of assessment
    C. Team composition
    D. Facility characterization
    E. Critical asset description
    F. Summary of threat assessment
    G. Vulnerability assessment objectives
    H. Summary of conclusions
    I. Summary of recommendations
III. Background
    A. Scope of assessment
    B. Facility Characterization
        1. Organizational mission
        2. Criticality of the facility
        3. Key staff
        4. Major functions
        5. Geographic location
        6. Overall physical characteristics and conditions
        7. Significant features, including history
        8. Occupant information
        9. Community demographics
        10. Supply chain and transportation system
        11. Specific critical assets
        12. Security policies and procedures
        13. Regulatory and legal requirements
        14. Reviewed facility blueprints, site diagrams, and floor plans
        15. Identification of property boundaries
        16. Location of authorized access points
        17. Maps depicting facility ingress and egress paths
        18. Descriptions of physical structures
        19. Traffic patterns
        20. Neighboring facilities

- C. Assessment Overview and Process
  - 1. Identification of critical functions
  - 2. Significant threats
  - 3. Available documentation
  - 4. Vulnerability assessment team composition and biographies
  - 5. Schedule

IV. Major Vulnerability Areas
- A. Site
- B. Environmental
- C. Structural
- D. Physical Protection Systems (PPS)
- E. Policies and procedures
- F. Documentation
  - 1. Security plans
  - 2. Security incident reports
- G. Security personnel
- H. Life safety and fire protection systems
- I. Communications systems
- J. Information technology security systems

V. Conclusions

VI. Recommendations
- A. Prioritized ranking of recommendations
- B. Cost-benefit analysis of recommended changes

VII. Appendices
- A. Facility and area photographs
- B. Blueprints
- C. Site diagrams
- D. Floor plans
- E. Security survey checklist
- F. Cost-benefit analysis documentation

This page intentionally left blank