SAND2000-3014C

Sandia National Laboratories

Security Systems and Technology Center

An Overview of the Vulnerability Assessment Process for Fixed Sites and Transportation

DISCLAIMER

DISCLAIMER

Portions of this document may be illegible in electronic image products. Images are produced from the best available original document.

Introduction

Considerations in Conducting a Vulnerability Assessment

Background

Vulnerability Assessment methodology developed for fixed nuclear sites has proven to be extremely effective in assessing associated transportation issues. The basic methods and techniques used are directly applicable to conducting a transportation vulnerability assessment. The purpose of this paper is to identify those areas of the vulnerability assessment that are common to fixed-site locations and transportation. Additionally, special areas of consideration when conducting a transportation vulnerability assessment will be identified.

Vulnerability Assessment

Conducting a vulnerability assessment involves a systematic process of:

Threat Characterization

- In characterizing the threat, the analyst must determine the type of threat that may exist. To define the threat the analyst should identify the type of adversary that could be involved, their tactics, objectives, motivation factors, capabilities, and limitations.

- The types of threat could include: outsiders (terrorists, criminals, extremists), insiders (hostile employees, psychotics, blackmailed or threatened employees, or criminals), or a combination of insiders in collusion with outsiders.

- The type of tactics used by an adversary could include: force as an overt attempt to overcome a security system by violence, stealth attempts to defeat a physical protection system by avoiding or manipulated internal components to prevent detection and deceit as an attempt to defeat a security system using false identification or authorization.

- Potential threat objectives include: misappropriations (theft), and sabotage. Nuclear theft is defined as the illegal act of removing material, equipment or components involved in processing nuclear related components or devices. Sabotage acts by an adversary are designed to cause harm to materials, equipment, facilities and personnel.

- The adversary's motivations can range from economic, ideological to personal. The adversary may be strictly in it for the opportunity to gain financially or their ideological/political philosophies drastically vary from the accepted norm. Personal desires such as: a need for revenge, or mental instability may motivate the person to act irrationally.

- When determining the threat capabilities, the analyst should consider: the number of adversaries, their roles (insider/outsider) , type of weapons and equipment, work

capacity and ability to carry equipment, available transportation, type of knowledge and skills required, and any collusion activities.

- In identifying the types of limitations possessed by the adversary, the analyst is able to realistically assess the data and provide a clearer definition of the threat that exists. Based on the type of facility, the analyst can determine in advance the kind of planning required for the adversary to achieve the objective. The adversary's knowledge base is dependent on the amount of information known to him/her about the facility. A single target for theft may require a team of highly knowledgeable and trained adversaries, a desire to commit an act of sabotage may only require the action of a single individual.

- Information about the facility for the threat characterization can be collected from several sources: specific site engineering plans, physically conducting facility tours, perception of subject matter experts concerning physical protection matters, review of past incidents, intelligence, and identifying the attractiveness of the target(s).

Target Identification

Target identification is the basis for developing a physical protection system (PPS) and analyzing the effectiveness of the system. The target identification process consists of determining: consequences considered undesirable, concrete types of unauthorized actions, criteria and methods of analysis of technological processes, and determine established criteria and methods to analyze unauthorized actions.

- Consequences considered undesirable include a real threat of damage to the public health or to the environment as result of a radioactive release of material either through sabotage or the outcome of material theft. Economical and political damage may also be a consequence of such actions.

- Possible unauthorized actions which could lead to undesirable consequences include: theft, radiological sabotage, and industrial sabotage.

- When targets are identified as radiological, it is important to determine the level of radioactive release that would constitute a hazard. Consequences associated with sabotage of radioactive materials are determined based on the source of radiation, the location of the material, and release mechanisms. Nuclear material must be properly categorized to ensure that the appropriate physical protection measures are applied correctly in the assessment.

- Fault tree analysis is used to determine the combinations of events related to the actions of potential adversaries that could lead to undesirable consequences.

Facility Characterization

Characterizing the facility requires a methodical approach which allows the analyst full access to the facility, its technical drawings and related resources. This systematic gathering of information is used to develop a clear picture of the site. The facility characterization process involves: classifying structures, developing information sources, drawing facility diagrams according to target locations, identifying the present physical protection system and building adversarial sequence diagrams.

- When classifying structures, the analyst identifies site borders, transportation lines, building layouts, location of vulnerable areas, points of access and regress, and operating conditions as well as the type and time of shifts.

- Information sources could include site plans, documentation review of past incidents, interviewing facility management and employees. General maps indicating barrier locations and other physical protection systems should be available for review.

- Adversary sequence diagrams are developed to identify an adversary's path into a facility. Adversary regress is important as well, due to the threat of both the insider and outsider. Once the path is identified the physical protection system is analyzed to ensure effectiveness.

Scenario/Strategy development

In developing scenarios and strategies for evaluating an adversary's attack on a facility regardless of their goals and objectives, it is incumbent upon the analyst to place himself or herself in the position of the adversary. Questions such as, "If I wanted to take material from this facility or commit an act of sabotage, what do I have to do to be successful?" need to be asked. Hypothetical situations should be presented for thought and shared among others working on the assessment. The information discussed in the previous sessions will help in developing adversarial scenarios and strategies used to defeat physical protection systems.

There are five terms used primarily in scenario/strategy development: strategy, path element strategy/tactic, defeat method, scenario, and path.

- **Strategy** refers to the overall method planned by the adversary to achieve the objective. An example of a strategy might read, "Conduct a covert attack on a facility at night using one protective force supervisor in collusion with the adversarial force."

- **Path element strategy/tactic** refers to a method used to defeat a path element. A path element strategy/tactic could include disabling physical protection systems as necessary, to perform covert actions.

- The **defeat method** is a means to prevent a safeguard in a path element from accomplishing its purpose. An example of a defeat method for a detection system could include bypassing the essential mechanisms that make it function properly.

- The **scenario** is an outline of the sequence of events an adversary plans to take to achieve the objective. The scenario is the final product of the entire piece put together to determine the actions an adversary would take to be successful.

- The term **path** refers to the physical route taken by an adversary to achieve the objective. Direction and type of obstacles encountered describe paths.

Adversary Planning

There are three levels associated with adversary planning: adversary strategy, element strategy/tactic and defeat method. **Adversarial strategy** focuses on the three primary functions of a safeguards and security system: detection, delay and response.

- Detection involves determining that an unauthorized action has occurred or is occurring. Detection includes sensing the action, communicating the alarm to a control center, and assessing the alarm.

- The delay element of a physical protection system is designed to impede adversary penetration into or exit from the protected area.

- The response element is designed to counteract the adversary's action through engagement and neutralization. As an analyst playing the role of the adversary you want to find ways to circumvent these physical protection elements by preventing detection, disabling delay systems and diverting or confusing response forces.

Analyze each function by focusing on supporting safeguards and security systems. Subject matter experts can help educate you on component knowledge and the best way to defeat each system. Each threat should be analyzed to include both the outsider and insider. As the analyst you should understand the differences associated with varying states of the facility, such items as: daytime vs. night-time, normal duty hours vs. off-hours, and stationary material vs. material in transit. The focus of the analysis can change based on the measure in place. Material control and accountability for vault custodians is an appropriate measure for an insider, but may not be an appropriate measure for the terrorist.

Facility state is also important when considering ways to bypass system delays. Delays that are inactive during certain periods of the day can include: vault doors, gates and other open access areas. Custodians may defeat delay by access, authority or by waiting, whereas the terrorists may focus on destroying it.

In evaluating the response element you want to determine the command and control structure of the response. There are several common command and control components, which include: alarm acknowledgment, visual assessment through CCTV or patrol response and tactical deployment. In evaluating the effectiveness of each of these components the analyst assesses such things as training, policies and procedures involving alarm response, and weaknesses in tactical deployment.

An **element strategies/tactics** list is developed to identify the adversary strategies, facility states and possible defeat methods that might be employed at a safeguard by an adversary. Identifying a list of this nature can help determine which strategies/tactics are consistent with the type of adversary being assessed. This includes non-violent custodian vs. terrorist. Documentation of the process is important, because it helps eliminate duplication of strategies/tactics and presents a clearer picture of the purposed adversary's actions. Documentation should include: a description of the strategy/tactic being employed, the type of force, deceit or stealth and adversary characteristics such as motivation for their actions. A well documented scenario is easily recreated should the analyst be required to present the information in the future.

To understand the **defeat method** of a system it is essential to know how the safeguards and security method functions. Defeat methods can best be explained through a practical set of examples as illustrated. As you know, the function of a detection system is to sense unauthorized conditions, communicate the alarm and assess the alarm. Defeat methods could then include: bypass, spoof, and tamper; jamming and tampering; and stealth and deceit. The delay function could include such items as barriers, which an adversary could defeat through penetration. The response is accomplished through the use of a protective force, which could be defeated by diversion techniques or totally disabled by being out numbered or out gunned.

Developing Scenarios

A well developed, realistic scenario is an adversary's recipe for success in achieving the objective. Scenario development is a combination of piecing together consistent adversary strategies, element strategies/tactics and defeat methods. There are three components to successful scenario development:

- Personnel - The personnel in the scenario should represent the type of threat being assessed. If a terrorist organization is the adversary and they have no insider assistance, how much information or intelligence can they realistically possess? What type, if any, special training would be required by the adversarial group?

- Equipment - Is the amount and type of equipment proposed by the adversary force available? How difficult would it be for the adversary to obtain specialized equipment to achieve the objective?

- Implementation - Is the scenario simple to carry out, or does it involve extensive amounts of equipment, specialized adversary training and a complex attack plan? Plausibility increases if the scenario is relatively simple to implement.

Insider Evaluation Approach

The term "insider" is used to describe an individual(s) with privileged knowledge of and/or access to a facility or location. Facilities handling nuclear materials and other attractive targets must take into consideration the threat of an insider. The insider possesses traits similar to the outside adversary or external threat, but differences in their level of knowledge, access and authority increase the likelihood for success.

Types of Insiders

Specific types of insider information may include: knowledge of security force work schedules and posts, building layouts and locations of detection and denial systems or they have authority over others and can use that authority to even gain additionally not personally known. They can select the time and strategy to be successful in their mission . The common types of insider crimes include: theft of nuclear materials or parts, theft of classified information, and sabotage.

There are several types of adversaries involved in committing these crimes. The first type of adversary is the criminal offender , who in most cases has a prior history of committing criminal acts. The two most prevalent crimes in the world today are the solicitation and trafficking of illegal drugs and high tech computer crimes. A study conducted in 1988, nearly ten years ago, indicated that computer related crimes accounted for a $5 billion loss to businesses annually.

The next type of offender is the disgruntled employee. Typically, this is a person who has been employed in their position for several years, but who has become dissatisfied with the working environment around them. Even if the employee is not unhappy with their job, external influences can cause the employee to react negatively at work. The most common of these situations is an unhappy domestic life. With the increasing threat of downsizing organizations, which doesn't correlate to the workload increasing, employees often find the stress too difficult to take and act out toward management. A

study by the National Institute for Occupational Safety and Health indicates that the #1 killer of women in the workplace stems from some type of violence that occurs, and that violence in the workplace is the #2 killer of men. Other employee related problems can include drug abuse, and a wide range of psychological problems such as long term depression.

The anti-nuclear activist or what is commonly referred to as the ideologically motivated, believe so strongly in certain issues, that they are willing to defy legal convention for the sake of their beliefs. Ideological trust violators are typically bright individuals who possess a committed attitude toward a rebellious nature. They are often found to be people who in the organization represent a controversial issue, one that may cause people to react through protest.

Past Incidents

Past insider incidents indicate that insider criminals are among the most difficult and dangerous to defend against. Although financial gain is often the primary motivation, others factors contribute to the problem. Some of these other factors include: family relationships, disgruntled employees, and ideological allegiances. One single group of individuals represent approximately 41 % of the perpetrators in these cases, members of the protective force (guards). The protective force is probably one of the very few groups of individuals that have complete access to any place within the protective area and would not attract any suspicion based on their presence. Insiders acting alone can be extremely dangerous, but in cooperation with other insiders or external perpetrators the likelihood for success is multiplied.

In December, 1987, an American PSA Flight 1771, crashed and killed everyone aboard. The perpetrator was a former employee who had been fired from the airline for alleged misconduct. Although no longer an employee of the airline, he was able to use his access card to gain entry into the plane with a gun in his possession. Once in the air the ex-employee gained control of the cockpit and shot the crew. Shortly after the incident the Director of Security for the Federal Aviation Administration (FAA) was quoted, "*The most difficult problem (in personnel screening at airports) is those with knowledge and access.*" (Associated Press, 1987).

An example of a computer related incident involving a disgruntled employee took place in September 1996. A small Internet provider was virtually erased by the former employee who on the day he was laid-off from his job went into the company's files, to include backups and erased all the data.

In Germany a Slovak engineer was arrested on suspicion of smuggling 6 pounds of radioactive uranium into the country. The uranium was found in a bank safety deposit box in the southern town of Ulm. The 49 year man was arrested after a tip from Austrian police reported that the man was trying to sell the uranium for $1 million, US currency.

Characteristics of the Insider

There are two categories of insiders, passive and active. The passive, or non-violent insider's participation is limited to providing information about facility operations and safeguards to a colluding insider or outsider(s). The information available to the passive insider is only what he or she can readily obtain without fear of detection.

The active insider is willing to provide more than information to the adversarial group. This type of person is willing to open doors, provide hands-on help and aid in neutralizing protective force personnel. They will use all types of force, stealth and deceit tactics to minimize the likelihood of detection. There are two types of active insiders; violent and non-violent. Violent insiders include psychotics, and criminals, who may use force regardless of whether it enhances their chances for success or not. The non-violent insider has a clear decision criteria and optimizes his actions accordingly. The non-violent active insiders is not willing to be identified or risk the chance of engaging protective forces.

Insider motivation for committing these acts can range from their strong belief in an idea to a desire for monetary gain. Based on their motives, the insider will determine how far they are willing to go to accomplish their goals. A highly motivated ideological individual may be willing to kill or be killed to achieve their goal and not worry about being detected. Conversely, someone who desires financial gain as their primary motivation will probably use covert actions to avoid detection. Additionally, this type of individual will abort their plan if they believe the opportunity for detection is too great.

Insider Protection Measures

To be effective in protecting a facility or material from the threat of an insider requires a combination of several measures. First, there are human reliability program considerations. These programs focus on the initial employment screening process of applicants. Prospects for employment should be required to pass a drug screening test, background investigation and possibly psychological screening. Once the applicant has successfully met the requirements for a security clearance, the applicant should be directed to undergo security awareness training. Security awareness training will identify the individual's responsibilities in dealing with security related issues.

The second measure addresses physical security. Physical security can include, but is not limited to: barriers, intrusion detection systems, contraband detection, access controls, surveillance, protective force response and any contingency plans. Although physical security measures are primarily used to limit access and delay intruders, they can also deter the insider if they believe there is a high probability of being caught due to the physical security measure in place.

Other protection measures can include: material control and accountability programs, supervisor's observations of employee conduct, consolidation of inventories to reduce the number of targets and effective physical protection measures to monitor access and egress. education, physical protection devices, and policies and procedures ensuring appropriate handling and controls of attractive target materials.

Quantifying Effectiveness

To this point we have quantified effectiveness of physical protection systems through the use of subjective terms, such as low, medium, and high. In this section we will discuss in detail the use of detection probabilities to quantify safeguards effectiveness. Quantifying safeguards effectiveness is in important in determining the probabilities of success by an adversary to achieve its objective. Although, limitations to the process exist, quantifying offers the analyst several advantages which will be discuss in this session.

Qualitative Evaluation

There are two primary advantages in using qualitative evaluation in determining safeguards effectiveness.

- The first advantage is that the results allows the analyst to immediately identify any obvious or glaring vulnerabilities in the physical protection system.
- Secondly, any imbalance in the protection system is recognized quickly and corrective actions can be taken to reduce any deficiencies.
- Limitations to this type of evaluation include: imprecise communication based on subjective opinion, difficulties in combining qualitative descriptors, and the difficulties presented in comparing adversaries and strategies.

Interpretation of qualitative effectiveness is often difficult to understand when first attempting to apply numbers to probability of detection. Probabilities can be obtained from several sources: experimental data, site-specific performance tests and expert judgments. An example of experimental data can include information on system evaluation and testing performed by the manufacturer or independent testing sources. Site-specific performance testing is designed to remove the theory of application and evaluate the physical protection system in place as it is actually being applied. Subject matter experts can offer specific judgments as to the design and implementation of a system based on personal experience and knowledge.

Quantitative Evaluation

Quantitative evaluation has several advantages. First, it improves the communication process by assigning specific values to the probability of detection, so overall system effectiveness can be accurately computed.. It allows for comparisons between personnel and strategies. It helps in comparing various safeguards configurations and offers the ability to test alternative judgments.

In assigning probabilities the analyst should clearly define the "event" and assumptions. Interviews with subject matter experts should be conducted using proven interviewing techniques and documenting interview results. It should be noted that subject matter experts' opinion may vary and differences need to be documented. If possible, subjective judgments should be supported by empirical data. This data backup will support the decisions made. First test probabilities that:

- strongly influence evaluation results,
- are subject to differences of opinion,
- are associated with likely adversaries and strategies,
- and can be tested for accuracy inexpensively.

Additional Insider Topics and Insider Evaluation Summary

When considering the threat of the insider, it must be recognized that insiders can have the same motivations as outsiders. Any employee may pose a potential insider threat, even the most trusted plant manager or protective force personnel. It should not be assumed that since a person is an employee that he or she will be free from greed or job dissatisfaction and invulnerable to cooperating with adversaries as a result of coercion.

Up to now, discussion has concentrated on the types and characteristics of the insider threat, and the insider's exit from the target. We know that the path(s) followed by the insider is the basis for establishing a physical protection system that addresses the variables associated with the insider. The insider's path(s) is a combination of their access, authority, and knowledge of facility operations and information. Examples of insiders could include:

- a grounds keeper with no building access who steals a badge to enter the Inner Area,
- a protective force officer with no access to SNM material, but obtains the combinations and enters at night,
- a reactor operator who is part of a two-person rule, decides to covertly enter the reactor area during a break.

Consider Insider Entry

Looking at the possibilities for detection of insider actions during the entry path actually doubles the number of theft stages, due to the exit paths required, which may not be the same path. This is important when considering the insider whose desire is to commit an act of sabotage. Exit from the target may be totally undetected since removal of material is not the goal.

The analyst may develop scenarios that require the entry of contraband into the target area. In some cases, contraband can be obtained within the site. As an example, if an insider's goal is to remove material, he or she may need to smuggle in explosives to acquire the target then exit.

Collusion

Typically, insiders collude to decrease their probability of detection. Collusion helps the individual(s) gain access to the target area, usually together they can overcome the lack of authority, and obtain any knowledge of special requirements associated with the target and surrounding areas. An insider with an overall low probability of detection may avoid colluding with anyone.

Different types of collusion scenarios can be developed to allow insiders to work independently or jointly at each stage. An example of an insider working independently could include a worker who handles material. The individual could acquire material from the PA and hand it off to an accomplice outside the PA. The two-person rule is ineffective if the individuals are in collusion with each other.

To analyze the different types of collusion scenarios that can be developed, the analyst begins the process by examining the single insider results. Once the analyst has identified the different types of insider adversaries, a review of the layers on the optimal

path(s) where safeguards are most effective is conducted. A determination is then made as to the adversary types that are most capable of helping at the different layer(s). Any safeguards components and procedures which can be exploited by a colluding team should be identified.

In evaluating the effectiveness of a colluding insider threat, analysts should develop several manageable collusion teams. These teams begin working on combining attributes of each insider until they have created a "super adversary." Analysts then brainstorm strategies and assign detection probabilities. Documentation on each facility and system condition is then collected and used to further develop scenarios. Scenarios should be realistic and consistent. A Rand Corporation study (1990) indicates that more than half of the insiders (employees) who collude or in their words "conspire" are operational employees engaged in normal daily operations. The majority of the conspiracies involved coworkers and some even involved a large number of employees, such as employee/employer problems caused by poor moral.

Violent Insiders

In evaluating the violent insider the analyst can examine the nonviolent insider path(s). First, review the layers which provide the most detection for the optimal scenario. Now, look at each layer and brainstorm how violence could be used. Always consider the use of covert and overt violence, to include the facilities response to a violent insider(s). As an example, would responding protective forces recognize the insider as a "good guy" and ignore his actions until it was too late? The analyst may need to adjust entry path(s) to account for the probability of detection while smuggling contraband, violent insiders, and subsequent layers for expeditious exit form the area.

OUTSIDER EVALUATION

In this section, we will expand our characterization of the outsider and evaluate the various effectiveness of each type. Additionally, a full range of outsider attack information will be presented for use in evaluating the risks affiliated with an attack. The analyst should develop a clear understanding of the characteristics of the outsider and factors that motivate each individual(s). Questions to ask yourself include:

- What is the adversary's objective and motivation to achieve the objective?
- What tactics or actions will the outsider use to defeat physical protection systems?
- What level of access or authority does the outsider possess?
- Does the adversary have the ability to acquire the tools and skills to operate the required equipment to be successful?
- Does the adversary possess the required level of knowledge and is collusion a part of that knowledge?

Outsider Attack

There are some basic characteristics of an outside adversary attacking a facility. The outsider places primary emphasis on the use of:

- force and stealth, but deceit and collusion are always a possibility,

- stealth vs. access
- and number of personnel used and equipment vs. authority.

The outsider knows that they have a limited time span to accomplish the tasks and leave the area before detection. The following definitions will be useful in determining Conditional Risk: R=(1-Pe) x C:

Pe= Probability of System Effectiveness

C= Consequence of adversary act (0-1)

Probability of System Effectiveness =

Pe= Pi x Pn for outsiders and violent insiders

Pi= Probability of Interruption

Probability that detection occurs early enough that response forces can arrive to keep the adversary from completing the scenario. This is highly dependent on the response time of the protective force.

Pn = Probability of Neutralization

Probability that protective force response successfully defeats adversaries given that interruption occurs.

Facility Characterization

A detailed description of the facility's buildings, structures, modes of transportation, physical protection systems, and site conditions will help in developing a complete picture of a facility's strength and limitations. In this section we want to expand on the information concerning the facility characterization by identifying facility states, drawing a facility diagram which shows the adversary's paths and targets, describing safeguards and security measures, and collecting response time data.

A list of facility states is comprised of four areas:

- Operational conditions are listed as normal operations, non-operational, material (SNM) load/transportation, maintenance, and emergency operations.
- Status of the vault and gate operations are listed as open/closed.
- Shifts can be identified as day or off, day of the week, and holiday.
- Weather such as fog, rain, wind, or snow.

Facility states can vary depending on the facility being evaluated. Once the diagram is completed potential adversary paths are identified and annotated on the adversary sequence diagram. This diagram displays the most likely paths an adversary would take to commit an act of theft or sabotage.

In determining the protective force response the analyst should develop extensive documentation on command and control procedures, determine which protective force units or teams are responding and estimate the times associated with notification, communication, and deployment. Visualizing this information is best achieved by using a technique called "storyboarding." Storyboarding allows the analyst to layout a timeline of events and protective force response. Additional information can be added to the storyboard as it is discovered.

Response to different site conditions and protective force responses should be analyzed for each strategy.

Strategies and Scenarios

When developing strategies for the outsider the analyst looks at three areas:

- detection,
- delay,
- and response.

The path element tactics used in the outsider scenarios will be specifically designed to accommodate this type of adversary. As an example, an outside adversary may use several types of tactics to enter a portal, such as: deceit, stealth or force. The specific tactic involved could include a forged badge entrance during protective force shift change, sneaking through the portal, or conducting a full assault on the portal area.

Detection and Delay

Effective detection can be attributed to the process in which an alarm is received and the performance of the detection measure. In the detection process there are three key elements: alarm signal initiation, alarm report and alarm assessment. The measure of performance is a combination of the probability of detection, the amount of time required for communication and assessment and the frequency of nuisance alarms.

Delay measures are evaluated based on three processes: providing obstacles (natural), physical barriers (man-made) and protective force personnel. Each one of these processes individually can provide delay or combined can increased the desired delay times. Delay performance is measured by the time it takes to defeat the delay.

Barrier defeat times are determined based on the type of tool used against a particular barrier. As an example, take the use of high explosives vs. power hand tools. The delay times are quite different, and the probability for detection will probable increase with the explosives. When identifying delay characteristics it is best to document the following:

- types of tools to be used,
- the delay and detection curves for each tool,
- the weight, characteristics for delay, number of personnel and skills required, and tactical considerations.

A tactical consideration example may include the number of personnel required to perform an operation, who while performing the operation, are unable to shoot a weapon.

Example

In this example, *adversaries are required to enter a vault door (45 cm) within a facility.* Once the objective is established, the basic question is, "how does the vault door get opened?" First, the adversary can have someone else open the vault by overpowering facility personnel (force), attempt to covertly sneak pass facility personnel (stealth), or pose as an authorized employee of the facility (deceit). The adversary could get the keys and open the door by using similar means.

For this discussion we will concentrate on opening the door through the use of stealth and force. The vault door could be penetrated by "blowing the door" (force) or through quiet penetration by tampering with the intrusion system (stealth).

The vault door characteristics include:

- 45 cm thick concrete wall with rebar at 15 cm centers,
- interior motion sensors focused on shelves,
- combination lock and a padlock, both controlled,
- grid mesh sensor on the door,
- Balanced Magnetic Switch on the door, and Central Alarm Station communication required to place alarms in the access mode when the vault is entered.

In considering a forcible attack on the vault door we could use one explosive charge to open a man-size hole entirely through the wall or blow the concrete out of the hole with explosives and cut the rebar. In both instances, collateral damage inside the vault could complicate the adversaries situation.

In calculating the time required to defeat the concrete vault wall, each step in the process must be identified and time to complete each task established. In this scenario the steps would include:

- set-up charge,
- retreat,
- blow through the wall
- return,
- cut rebar (if required),
- and crawl through.

Remember to annotate the point where detection may occur either at the beginning or end of a step. Delay times for cutting tool tasks can be identified in the same manner.

Delay and detection working together are excellent ways to combat an adversary, but remember that delay before detection isn't a useful safeguard and assessment must be accompanied by delay. General observation and Close Circuit TV (CCTV) monitor surveillance are not as good as they might appear. Vigilante personnel are critical to successful detection.

Evaluating Response

The ability to effectively engage an adversary by a responding protective force is measured by Response Force Time (RFT). The RFT consists of the time to assess the alarm, the time it takes to communicate for a response and the deployment time. Neutralization of adversaries is illustrated by Probability of Neutralization, Pn. RFT is selected over a period time.

In determining the RFT, all times associated with assessment, communications and deployment should be collected and documented. Times should be storyboarded and tactical considerations applied as necessary. Once the storyboard is complete, adversaries should be given the advantage in achieving the goals.

The RFT can be lengthen or shorten depending on the effectiveness of communications or tactical preparation. Tactical preparation is understood as:

- planning - coordination with other units, and protection strategy,
- field training - ability to work together to enter a building as a team,
- and demonstrated ability to accomplish the task during training exercises.

Additional RFT Considerations

Other considerations the analyst should be aware of and include:

- additional time given to the adversaries due to protective force's inability to track movement.
- accurately identifying the point when responding forces effectively engage and impede adversaries movement,
- and selecting a random RFT, based on SME experience.

In determining the probability of neutralization (Pn) as it relates to RFT the analyst will should ask several questions. First, is the Central Alarm Station (CAS) and/or Secondary CAS in a hardened Security Command Center? Is the Security Response Force (SRF) stationed in the CAS, in the Protected Area? And, does the SRF respond to fixed locations supported by sandbag posts or other hardened structures?

Quantifying Effectiveness

Probability of effectiveness is represented by Pe. To determine Pe for a given scenario we look at the scenario's threat, target, and facility state to decide what is the lowest Pe over all scenarios. The scenario achieving Pe is referred to as the Critical or Most-Vulnerable Scenario. The global effectiveness of the facility's safeguards and security system is measured looking at the Most-Vulnerable Scenario(s).

UPGRADE ANALYSIS

Typically, upgrades are something that everyone would like to do, but the reality of the situation requires that specific questions be answered to ensure practical, cost effective upgrades are proposed and eventually implemented. The primary purpose for upgrading a physical protection system is the discovery of some weakness or limitation that exists in the system. Obviously, if the system was operating effectively there would be no need to upgrade. The analyst's responsibility is to ensure that limitations in the physical protection system and s clearly identified and reported.

Solutions

Determining the proper solution to eliminate or lessen a system weakness can often be identified by the subject mater experts who work in the facility or those who have knowledge of the various systems. Brainstorm sessions are helpful to find plausible solutions to the problems. Possible solutions should be tested for effectiveness and compared against each other to reduce future system problems.

Solutions should be applied to the base risk analysis results and evaluated on risk reduction, cost of implementation, and sustainability. There may be numerous solution options available, but the cost may be too high or the ability to maintain a new system impractical. Solutions can be categorized by the time frame required for implementation. Quick fixes can usually be done immediately, whereas, near-term (less than two years) or long-term (more than two years) require additional planning prior to implementation.

When selecting optimal upgrades, the analyst should consider the following:

- combine upgrades into logical packages/groups,
- model upgrades to ensure other systems are not adversely effected by the changes,
- develop cost estimates to include labor, construction, equipment, operational impacts and sustainability cost impacts (technician training, equipment replacement, etc.)
- and finally determine cost vs. benefit.

ALTERNATIVE EVALUATION METHODS

Successful vulnerability assessments are conducted using a variety of tools and techniques, many of which you learned in this program. There is a quote concerning the use of tools to complete a task, *"if the only tool you use is a hammer, everything starts to resemble a nail."* In this section we will review the different types of tools used to assist the analyst in conducting a VA. The options available include computer-based, and table-top analysis. Both are effective in evaluating physical protection systems and related components.

There are four types of computer-based analysis that can be used to assess a facility's vulnerabilities, commonly referred to as: EASI, SAVI, ET, and ASSESS. Each has established objectives and expected outcomes. In addition to the computer-based assessments, a table-top analysis can be conducted, as well as performing validation testing and receiving "expert" review from subject matter experts.

Computer-Based Systems

The following computer-based systems are used to assist the analyst in conducting a VA:

- Estimate of Adversary Sequence Interruption (EASI)- one path, one scenario analysis which calculates probability of interruption for outsider scenario.
- Systematic Analysis of Vulnerability to Intrusion (SAVI)- a global analysis which finds the most vulnerable outsider scenario.
- ET- a global analysis which identifies the most vulnerable insider scenario.
- Analytic System and Software for Evaluating Safeguards and Security (ASSESS)- a global analysis which identifies the most vulnerable path of different threats to include insider/outsider and collusion, threat objectives and protection strategies.

Tabletop Analysis

Tabletop analysis can be qualitative or quantitative, depending on the scope of the analysis. The type of threats modeled include active insiders, violent insiders and outsiders. Threat objectives can include SNM theft, radiological sabotage, and industrial sabotage. Protection strategies include containment with neutralization and denial with neutralization.

Validation

Whenever possible validation testing and expert advice should be used to evaluate the results of the VA. The most important VA tool available is the combined brain power of the team conducting the VA.

Transportation

Vulnerability Assessment Special Considerations

Background

Ground transportation security is more complex than that of a fixed-site. The same physical protection elements (detection, delay, response) are present, but the response force plays a dominant role in preventing the theft or sabotage of material. Transportation systems are continuously exposed to the general public whereas, the fixed site location by its very nature restricts general public access.

The material transportation system (MTS) can be considered a moving facility. The MTS may consist of several material transports and response force carriers such as military escort vehicles and railcars. The area surrounding the facility (transport mode) automatically changes as the transport moves throughout the designated route. The terrain can change from flat level ground to rolling hills or mountains in a matter of moments. In addition to the terrain variations, the transportation operation exposes the facility to various kinds of public domain to include urban and country settings. Each area offers advantages and disadvantages depending on the location of the facility at any given point along the route.

Vulnerability Assessment

Threat Characterization

In characterizing the type of threat involved in a MTS vulnerability assessment, the analyst can refer to the threat characterization information initially determined for the fixed site location, where the material is stored when not in transport. Potential threat objectives can include theft, and sabotage. The analyst should acquire the standard threat characterization information:

- Adversary tactics, numbers, capabilities, and motivating factors.
- The types of threat - insider, outsider, and collusion.
- Specific tactics that may be used against a moving facility (target).
- Any historical data involving attacks on moving targets - assassinations, hijacking and attacks on convoys. Information can be provided by subject matter experts on protection of convoys and shipments of similar materials.

Target Identification

When identifying the target the analyst should:

- identify the type of material being transported,

- categorize the material,
- determine its level of attractiveness,
- determine what quantity would be a desired goal,
- and determine the number of shipping casks.

If the target is identified as a radiological target, determining the level of radiological release becomes critical due to the location of the transport at the time of the release. The position of the MTS could be virtually anywhere along the route, which includes a large metropolitan area, a small urban town or the country.

Facility Characterization

In the case of a MTS the facility is the transport system itself. Characterizing an MTS involves:

- classifying the structure of the transport walls, ceiling and floor, by use of drawings and visual observation, and determining their relationship to the target material,
- identifying all physical protection systems, and operating systems of the central alarm station,
- building adversarial sequence diagrams based on the facility's characterization,
- reviewing in detail, routes, danger zones, scheduled stop locations and choke points,
- determining both adversary entry and exit paths to analyze the protection system,
- determining the speed and timing of the MTS, as well as the time/distance to stop,
- the types of transports used for material and response force, i.e. rail, roadway, air, or ship.

Scenario/Strategy Development

In developing scenarios or strategies to commit an act against a moving target the analyst must think beyond the established ideas used to act against a fixed-site location. Historically, an adversary's success greatly depends on the MTS being stopped at the time of the attack. A moving target is difficult to gain control of and predictability factors are lost. It should be noted that the response force also has a difficult task of defending adversaries during movement. Cover and concealment is strictly limited to response force accommodations and a safe egress is nearly impossible. When developing scenarios there are several states or conditions that a MTS could be in, they include:

- stopped at a scheduled (predetermined) location - day or night,
- stopped at an unscheduled location - day or night,
- rolling to a stop - day or night,

- moving - at various speeds,
- and through the different types of environments and terrain along the route.

Adversary Planning

Adversary planning focuses on three key elements: detection, delay and response. The response force may be the only initial detection mode available. This may be especially true during daylight hours and in good weather conditions. But what occurs if the aforementioned conditions are not present? The analyst then determines what other detection systems are available and what their effectiveness is in relationship to the total system. In railcar systems being designed the analyst may find sensor capability that enunciates to a response force railcar, providing an intruder warning.

In assessing physical protection system delays, the analyst must take into consideration the number of response force members immediately available. The number of additional response force members available at any given location along the route may vary as well as their response time. Each type of delay should be:

- identified and annotated for future reference,
- evaluated to determine defeat tactics and timing.

The response element is designed to counteract the adversary's actions through engagement and neutralization. The analyst should brainstorm the type of tactics to be used to eliminate the response force. In a fixed-site location the exact location of protective force personnel at any given moment may be difficult to assess. The same freedom does not exist for a protective force restricted to specific locations such as a security force railcar or motorcade (convoy) configuration..

The primary response force (PRF) is described as that force immediately available to respond to an encounter with an adversarial force. Their primary objective is to deny access to the material. Adversary's want to know:

- the number of protective force members in the immediate response team and their location in the MTS,
- whether or not they have hardened fighting positions,
- type of weapons available to them,
- survivability to weapons and explosives,
- and deployment tactics.

The next question the analyst asks concerns the availability of a secondary response force (SRF) to reinforce the PRF and assist in denying adversaries access to the material and help prevent the removal or sabotage of the material. The primary differences that could exist between the PRF and SRF is:

- the number of personnel involved,

- location in relationship to the MTS,
- mobility issues (vehicles/second train/aircraft)

Lastly, the analyst should identify what type of law enforcement and military response exist within a few hours away from the incident site. Again, this may be difficult to specify since the MTS could be anywhere along the route when the incident occurs. When reviewing the route selected the analyst should annotate:

- location of law enforcement and military forces along the route,
- location of any forces that may be on training maneuvers,
- tactics used for a recovery/recapture operation,
- and mobility factors for additional response force members.

In assessing the defeats methods used by an adversary the analyst considers the elements of detection, delay and response. Although, the elements are the same for a fixed site location, adversary methods vary due to the variations presented by the MTS. In detecting an adversaries' approach to a fix-site location, a protective perimeter may be used with manned portals for access and egress. Detection of adversary actions for an MTS is usually provided by response force personnel. In those instances, where the mode of transportation is equipped with sensor capabilities, detection may occur at the outside shell of the vehicle itself. If detection does not occur until the shell of the vehicle is attacked, then delay becomes critical to interrupting the adversaries successfully.

If a limited delay time exists for the adversary to acquire the target, then detection before the attack becomes critical to response force success. Early detection of adversary actions can be accomplished through the use of an aggressive surveillance detection program. A program of this nature includes: periodic route surveys, identifying choke points and danger zones, intelligence gathering, etc.

Delay times for penetration of the vehicle are determined based on the amount of protective material (armor) available and the task times associated with penetrating the shell. When people are the material being protected, the adversaries' objectives must be clear to the response force. If kidnapping is the goal, then all the armor available will not be effective if the doors aren't secure. If assassination is the goal, then the shell should be designed in to prevent penetration by weapons and explosive devices.

Defeating the response force can be accomplished through a series of acts, which include: ambush, overwhelming adversary numbers, pre-positioned explosive devices, etc. The response force training program should include practical exercises on these types of issues.

Developing Scenarios

In developing scenarios for an MTS, the analyst must have a clear understanding of what it takes to make a scenario successful. Scenarios should be designed to replicate the actual threat presented. If "theft" of material is the worst case, then the scenario requires the adversaries to have an attack position, with time allocated for material acquisition, and allow for egress. If the worst case is sabotage of material, then simply pre-

positioning an explosive device with remote detonation may be all that is required to begin developing the scenario

In identifying adversary personnel the analyst should develop a design basis threat (DBT) statement. This statement indicates, based on similar past incidents and subject matter expert opinions what type of adversary would conduct a particular type of attack. In addition to the type of adversary, the statement would identify the most common number, capabilities and modus operandi. The number of adversaries vary depending on their goals and objectives, i.e. sabotage vs. theft. Analysis of past incidents and intelligence information is critical in developing crediable scenarios.

Next, the scenario should describe the type of equipment the adversary would need to accomplish their objective. Equipment could include: light and/or heavy weapons, hand and power tools, diversionary items like construction crew barriers and vehicles for egress. In addition to the DBT identifying the number of adversaries and equipment, the difficulty factor of their use and ability to acquire them is included.

Finally, the analyst determines the plausibility of the scenario. Is the scenario realistic enough to be considered in the analysis? A general rule in developing MTS (actual any scenario) is to keep it simple to implement.

As an example, the assassination of Israeli Prime Minister Yitzhak Rabin is a case in which the Arabs were thought to be the highest priority in security. A clearly defined DBT would have identified the most likely assailants to include both Arabs and Israelis. The Shin Bet (protective detail) was well aware of a known radical group of Jews who were against the Prime Minister's peace efforts with the Arabs.

It was determined that security on the outer perimeters were "tight" but security close to the Prime Minister was lax . The assailant gained access to the stage area by deceiving a security officer posted at the entrance. The assailant observed the officer and quickly displayed an identification card, stating " It's okay, I was here before." When questioned by authorities, the officer said he had no reason to question the man because he was a Jew.

Insider Evaluation

In considering the type of insider involved in an MTS, the analyst should identify those individuals with knowledge of convoy routes, schedules, denial systems and the type and quantities of targeted material. This may include material custodians at either the shipping or receiving ends, material handlers, security force personnel and management. The insider typically has the luxury of selecting the best opportunity for success. If the insider is acting in collusion with outsiders a set timetable may be established and followed.

Common insider objectives include: theft of material and proprietary information, extortion, kidnapping, revenge and sabotage. The criminal insider is the most prevalent today. The assassination of an American businessman in Russia is an indication of the old adage that criminals can not be trusted. The businessman hired Russian bodyguards to protective him, many of whom, were known criminals. As the assassination took place, "bodyguards" stepped out of the assailants way and allowed him to kill the intended target. Of course, no one could describe the attacker.

The disgruntled employee and ideological trust violators follow the criminal element as the most likely insiders. Each has their own motivations and should be included on the list of potential insider adversaries.

When evaluating the insider, the analyst develops an insider table that indicates the position the individual holds, access to material or principal, the level of knowledge possessed, access to vital security systems and opportunity for collusion, theft, and sabotage. Once the table is complete, the individual's categories are labeled as low, medium, or high. As an example, a shipping manager's knowledge of the type and quantity of material may be high, but his access to route information may be low, unless he colludes with the transportation dispatcher.

Past Incidents

MTS cases are available for nearly any type of scenario. As an example, the US Department of Energy studied attacks that have occurred on armored vehicles carrying money. Research indicated that in most cases the adversaries had either the aid of an insider or spent considerable time conducting surveillance and gathering intelligence on the organization's operation. Additional research conducted by several international transportation associations indicates, that employees who act as insiders often hold positions of authority, with knowledge of routes, materials being shipped, and security systems being employed.

Summary

As discussed, the Vulnerability Assessment process is a systematic means to evaluate the physical protection systems at a given location, and has direct applications to the various modes of transportation. It is imperative that the analyst understands that differences do exist and should be considered, but by following a proven process it creates a comprehensive report, that is defensible, as well as practical and understandable. A report that future improvement decisions and financial expenditures can be based upon.