Chapter 6

Risk Assessments

In this chapter . . .

- Definition
- Risk Assessments
- Qualitative Risk Assessments
- Quantitative Risk Assessments
- Specialized Risk Assessment Methodologies
- Risk Mitigation
- Risk Assessment Report

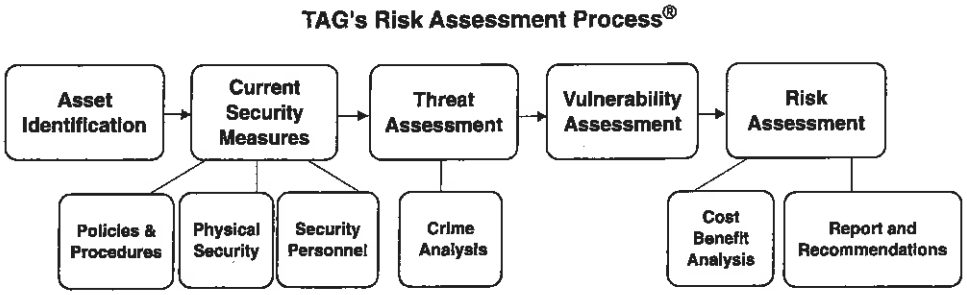

Figure 6-1
Strategic Risk Assessment Process, Copyright ©2007 by Threat Analysis Group, LLC. Used by permission. Additional information available from Threat Analysis Group, LLC via www.threatanalysis.com.

Definition

The risk management process involves assessing threats, vulnerabilities, and risk, evaluating and selecting security measures to reduce identified risks, and

implementing and monitoring the selected measures to ensure that the measures are effective. Risk management is truly a management process, whereas a risk assessment is simply a component of that continual management process. For many organizations, risk management involves much more than security functions and also includes insurance and legal issues.

Risk is a function of threats and vulnerabilities. It is the possibility of asset loss, damage, or destruction. Risk is the result of the likelihood that a specific vulnerability of a particular asset will be exploited by an adversary to cause a given consequence. A risk assessment is a quantitative, qualitative, or hybrid assessment that seeks to determine the likelihood that an adversary will successfully exploit a vulnerability and the resulting impact (degree of consequence) to an asset. A risk assessment is the foundation for prioritizing risks in order to effectively implement countermeasures.

No organization is without risk. The risk assessment and management process seeks to reduce risk to a tolerable level. The risk assessment is the culmination of the previous steps discussed thus far beginning with identifying assets, inventorying existing security measures, defining threats, and identifying vulnerabilities. The final step of the process is to calculate risks and make recommendations to reduce them to a level acceptable to the organization. Reducing risk involves identifying countermeasures that can mitigate vulnerabilities through the implementation of additional security measures or changing security measures. Cost estimates and cost-benefit analysis are key to selecting effective and reasonable security measures. Once the proposed recommendations have been selected, risk is recalculated to determine whether the risk has been reduced to an acceptable or tolerable level. Remember, no organization is without risk.

> ***The first step in the risk management process is to acknowledge the reality of risk. Denial is a common tactic that substitutes deliberate ignorance for thoughtful planning.***
>
> ***—Charles Tremper***

Recapping the risk assessment steps may be a good idea at this point. Identifying assets is the first step. This is the process of determining which assets are critical to the mission of the organization. Assets include people, property, and information. Critical assets are necessary for the organization to carry out its mission, for without them, functions and processes will fail and cause the mission to fail. The higher the consequence from the loss, damage, or destruction of an asset, the more critical it is. Each organization has different mission-critical assets; thus, no specific list is provided in this text. It is up to the risk assessment team to identify the critical assets of a particular organization. Critical assets are typically determined through interviews and questionnaires of the people charged with carrying out the organization's mission. For the Coca-Cola Company, the formula for Coke is a critical asset as it gives Coca-Cola a competitive advantage. For a litigator, his win-loss record is a critical asset. For

an athlete, her strength, agility, and energy are critical assets. For the security consultant, his integrity is a critical asset.

When determining the criticality of an asset, it is important to consider the time and money needed to replace the asset. Reputations may be a critical asset and take a considerable time to develop and replace after negative publicity. A company whose critical assets include their computer network may be able to replace the functionality of that asset rather quickly but with considerable expense. A homeowner whose house is destroyed by fire may be covered financially by insurance (risk transfer), but the time to build or buy a new house may be problematic. A manufacturing firm whose equipment is damaged may suffer downtime until the equipment is restored or replaced. The airport whose metal detectors unknowingly malfunction, though not a terrible development in and of itself, can be detrimental to homeland defense through cascading effects. Here again, asset criticality can be categorized quantitatively by value, replacement cost, and so on, or qualitatively by low, medium, high, or some other relative scale.

The second step of the risk assessment process is to inventory existing security measures designed to protect assets. The measures may include policies and procedures, physical security equipment, security personnel, or some combination of these measures. It is important to remember that security measures should not be assumed to be effective in protecting the assets. There are two effective methods for inventorying current security measures: inside-out or outside-in. In the outside-in approach, the assessment team begins at the facility's perimeter and works its way in toward the asset through each line of defense. The inside-out approach is the opposite with the team starting at the asset and working its way out to the perimeter. In addition to these methods, the inventory process should also include reviewing any available security documentation, including security plans, policies and procedures, the security officer's post orders, and physical protection system documentation.

The third step in the risk assessment process is the threat assessment, whereby threats are identified, characterized and rated on either a qualitative or quantitative scale. Threats are an act or condition that seeks to obtain, damage, or destroy an asset. The most common form of threat assessment is crime analysis. Adversaries can include insiders, outsiders, or a combination of insiders and outsiders. Adversarial capability and motivation should be assessed based on the adversaries' ability to steal, damage or destroy critical assets. The adversaries' past methods, equipment, skills, and training should be clearly articulated in the assessment report. Target attractiveness is a key component of the threat assessment.

The fourth step of the risk assessment process is the vulnerability assessment wherein weaknesses in the security program are identified via the vulnerability assessment's primary tool, the security survey. Vulnerabilities are opportunities. They are weaknesses or gaps in a security program that can be exploited by threats to gain unauthorized access to an asset. Vulnerabilities may be

structural, procedural, electronic, and human and provide opportunities to attack assets. Existing security measures may or may not address the security program's weaknesses. Vulnerabilities may also be classified quantitatively or qualitatively.

Risk assessment, including the cost-benefit analysis and report with recommendations, is the fifth and final step in the risk assessment process.

RISK ASSESSMENTS

Risk assessments are comprehensive and rational reviews that offer a logical and defensible method for security professionals to make decisions about security expenditures and to select cost-effective security measures that will protect critical assets and reduce risk to an acceptable level. Assessing risk is a dynamic process that involves continuous evaluation of assets, threats, and vulnerabilities. Risk assessments are typically a staged process whereby critical assets are identified, current countermeasures are enumerated, threats are identified, vulnerabilities are defined, and prioritized recommendations are made to protect critical assets based on probabilities of attack.

Risk assessments can be both quantitative and qualitative, or a hybrid. Qualitative assessments are based on the data available and on the skills of the assessment team, while quantitative assessments utilize numeric data to evaluate risk. Hybrid risk assessments utilize quantitative data where available and qualitative where metrics are not readily available or insufficient. While assessing risk is more art than science, the risk assessment methodology should be structured so that the results and recommendations can be replicable given a different assessment team. Risk assessments should generally be quantitative to the extent possible, recommendations for additional security measures should be the result of a cost-benefit analysis, and measures should be benchmarked against industry standards.

QUALITATIVE RISK ASSESSMENTS

Qualitative assessments are normally used when the assets in need of protection are of lower value or when data is not available. Qualitative risk assessments may also be used when insufficient historical information or metric data exists, precluding a quantitative approach. The results of qualitative assessments depend on the assessment skills of the people involved in the assessment. Risk levels are normally given in abstract values such as high, medium, or low, or color coded like the Homeland Security Advisory System. The American Society for Industrial Security—International released a security guideline entitled "General Security Risk Assessment" in 2003 which outlined one approach to qualitative risk assessments. The full qualitative approach is included at the end of this chapter.

Quantitative Risk Assessments

Quantitative assessments, on the other hand, are metric based and assign numeric values to the risk level. Overall risk levels are derived from all available security metrics. In physical protection systems, for example, the metrics used in determining the risk level include the threat level, probability of detection, delay times, and response force times. Quantitative assessments are commonly used for the protection of business critical or high-value assets. It should be recognized that security risks are notoriously hard to measure quantitatively because they involve human actions.

The general methodology for quantitative risk assessment is to consider the probability of an attack and the expected impact on each critical asset. The probability of attack is based on the adversary's motivation, capability, and intent. Depending on the type of facility or assets being protected, historical data may also be considered, but a lack of history should not be indicative of a low or nonexistent threat level. One reason a lack of history cannot be used is evident in the September 11 attacks. Had history been the only factor considered, the threat level would have been zero since no similar attack had occurred previously in the United States or anywhere else in the world. Vulnerabilities are calculated using the probability that each specific vulnerability will be exploited by an adversary. Based on the threat and vulnerability calculations, the overall risk level is calculated. In most situations, especially during an initial risk assessment, the risk level will not be acceptable. Thus, security measures must be identified, cost-benefit analyses performed, and the risk recalculated based on the theoretical implementation of these countermeasures. Only after a security mix has been identified and brings the risk level to an acceptable level will the actual implementation begin. In some cases, a phased approach may be used wherein the security decision maker implements certain security measures, allows some time to pass, and then conducts another assessment to see if the measures are effective in reality. If they are not, the next phase of measures is deployed and reassessed. This is similar to the pretest/posttest method used in the scientific and research communities.

The American Society for Industrial Security—International includes a quantitative approach to risk assessments in its General Security Risk Assessment guideline. (The quantitative approach is included at the end of this chapter in its entirety.)

RISK = THREAT + VULNERABILITY

Specialized Risk Assessment Methodologies

A number of specialized risk assessments exist that address the needs of particular industries or specific threats or types of critical assets. Among these specialized risk assessments are:

- The American Petroleum Institute's Security Vulnerability Assessment Methodology for the Petroleum and Petrochemical Industries
- The National Institute of Justice's A Method to Assess the Vulnerability of U.S. Chemical Facilities
- Sandia National Laboratories Security Risk Assessment Methodology for Water Utilities (RAM-W™), for Chemical Facilities (RAM-CF™), for Communities (RAM-C™), for Transmission (RAM-T™), for Prisons (RAM-P™), and for Dams (RAM-D™)
- The American Society for Industrial Security—International's General Security Risk Assessment Guideline
- The Federal Emergency Management Agency's Reference Manual to Mitigate Potential Terrorist Attacks against Buildings
- The Center for Chemical Process Safety's Guidelines for Analyzing and Managing the Security Vulnerabilities of Fixed Chemical Sites
- The National Institute of Standards and Technology's Risk Management Guide for Information Technology Systems
- Microsoft's Security Risk Management Guide
- Threat Analysis Group's Risk Assessment Methodology
- The National Fire Protection Association's Guide for Premises Security (NFPA 730)
- Sandia National Laboratories' Risk Assessment Method—Property Analysis and Ranking Tool (RAMPART)
- The Illuminating Engineering Society of North America's Guideline for Security Lighting for People, Property, and Public Spaces (IESNA G-1-03)
- The United States military's CARVER Methodology (Criticality, Accessibility, Recoverability, Vulnerability, Effect, Recognizability)
- The United States Air Force's DSHARP Methodology (Demographics, Symbology, Historical, Accessibility, Recuperability, Population)

Take calculated risks. That is quite different from being rash.
—General George Patton

Risk Mitigation

Risk management is the process of anticipating future losses and using risk mitigation strategies for reducing or eliminating that risk. Generally, five strategies may be employed to deal with risk: avoidance, reduction, spreading, transfer, and acceptance. Risk avoidance is an extreme measure since it hampers business. An example may be a department store that chooses not to stock a

particular brand or style of basketball shoes which are stolen with great frequency. Risk reduction is typically the driving force for security departments whose role it is to provide protection for assets. Risk spreading is a strategy used in moving assets to different geographic areas so that if one area is attacked, the consequence is limited to that area. In today's business climate, critical documents and information are commonly available electronically. Many companies store these electronic information documents in multiple locations so that if an attack were to occur, a backup of the information would exist. Risk transfer is a strategy used to remove the risk from the owner to a third party. Insurance is the best example of risk transfer in that the business hires the insurance company to assume the risk for a fee. Risk acceptance is another strategy used in mitigating risk. As the name implies, risk acceptance is simply where an organization assumes the risk to an asset.

Given a specific threat, many specific risk mitigation strategies are available to the security decision maker. Cost effectiveness is a key component in selecting the best one for the protection of assets. A thorough risk assessment allows security decision makers to prioritize risk reduction activities and adapt to changing and emerging threats. Risk mitigation is a security strategy that is accomplished by decreasing the threat level by eliminating or intercepting adversaries before they attack, blocking opportunities through enhanced security, or reducing the consequences if an attack should occur. Without question, the best strategy for mitigating risk is a combination of all three elements: decreasing threats, blocking opportunities, and reducing consequences. This is the homeland defense strategy used by the United States government and many other governments across the globe in the War on Terror. The United States' homeland security strategy may be characterized as the three P's: Prevent, Protect, and Prepare. The Department of Homeland Security's strategy is to reduce the threat by way of cutting terror funding, destroying terrorist training camps, and capturing terrorists; to block opportunities through enhanced security measures such as increased airport and maritime security; and to reduce the consequences through target-hardening efforts that minimize damage such as window glazing and through shortening response and recovery times.

For the security decision maker, specific countermeasures are available for each P. Prevention measures can include psychological measures designed to deter criminals from perpetrating their acts on a given property by increasing the risk of detection and capture. Protection measures include security personnel and vaults. Preparation measures include alarm system monitoring services that respond to alarms. More than one security measure may exist to protect a given asset. As such, for each potential security measure, the risk reduction benefit should also be assessed quantitatively or qualitatively. The measure selected may not necessarily be the most effective; rather, it is preferable to select a cost-effective measure that brings the risk down to a tolerable

level. As is often the case with security measures, the sum is greater than the parts in that multiple security measures working in conjunction with one another can reduce risk to an acceptable level. Similarly, one security measure may protect more than one asset. In either case, the overall effectiveness of security measures should be assessed to determine their net effect.

As defined above, security measures that provide maximum protection often come at a high price. While maximum protection may be warranted in certain critical infrastructures, it is not the standard for most industries. The typical standard is reasonable. Defining a reasonable level of protection to provide for the protection of people, property, and information is the primary task of most security decision makers. The problem with this standard, however, is that reasonable minds may disagree. Another security strategy is the concept of balanced protection, which simply means that no matter how an adversary attempts to reach the asset, security measures that deter, detect, or delay his advance will be encountered. Balanced protection is accomplished through yet another security strategy called protection in depth. Protection in depth is also known as security layering wherein the asset is behind multiple layers of security measures, each requiring penetration in sequence to reach the asset.

Regardless of whether maximum or reasonable protection is required, the cost of each security measure must be determined. Security equipment costs include initial costs, training costs, and ongoing maintenance and repair costs. Security personnel costs include background checks, training and continuing education, uniforms, equipment, and licensing. The rule of thumb for the selection of security measures is that their total cost should not exceed the cost to replace or repair the asset being protected. Another strategy used in the protection of assets is to provide protection only for critical assets, with the anticipation that other assets will be secured through a diffusion of benefits. Diffusion of benefits will be discussed in detail in the prevention chapter.

Risk Assessment Report

The risk assessment report is a comprehensive written document that incorporates all elements of the risk assessment methodology. Typical components of a full-scale risk assessment report include a listing of major assets, critical assets, and the facility characterization, a summary of existing security measures, the threat assessment report including supporting documentation with crime analysis charts and graphs, major elements of the vulnerability assessment report with the security survey included as an appendix, and recommendations for security modifications with the cost-benefit analysis. The goal of the report is to highlight the findings of the risk assessment so that those who hold the purse strings are able to make educated risk mitigation decisions that may include one or more of the five risk mitigation strategies (avoidance, reduction, spreading, transfer, and acceptance). The following suggested format builds upon the format used for the risk assessment report.

Table of Contents

The table of contents in a risk assessment report should identify each major section and subsection and be identified by page number.

Executive Summary

Similar to the vulnerability assessment report, the executive summary of a risk assessment report is an overview document used to provide a condensed version of the entire report and highlights key issues for decision makers who do not have the time to read the full report. The executive summary should not be longer than 10 percent of the full report and is often much shorter and should suffice as a stand-alone document. The executive summary should list the major assets and critical assets, and should include the facility characterization. It should also summarize the existing security measures, the threats posed to the assets including the relevant information from the crime analysis, and the major vulnerabilities. The executive summary should conclude with the recommendations and a call for action.

Background and Methodology

The background and methodology section of the risk assessment report outlines the scope of the risk assessment and defines the methodology. The methodology may be specific to the facility or organization, an industry-specific methodology, or a general methodology. Assessment team members should also be identified along with their credentials in this section of the report. The facility characterization and security inventory are discussed along with the security philosophy of the organization, if one exists. Historical attacks will also be included in this section, along with a general threat overview. Vulnerabilities uncovered during the security survey are outlined, along with any interim remedial measures designed to deter, detect, or delay immediate threats.

Assets and Critical Assets

This section outlines the facility's assets and critical assets, with special attention to defining the extent to which assets are necessary for critical functions or which assets are of a mission-oriented nature.

Existing Security Measures

This section of the risk assessment report contains a discussion of the current security policies and procedures, the existence of any security manuals and post orders, types of physical security measures in use at the facility, and documentation concerning the use of armed and unarmed security officers or

off-duty police officers. The scheduling practices are of utmost importance in the security personnel discussion, along with hiring standards, background investigation procedures, post orders and training provided, patrol practices, security incident reporting procedures, and equipment and uniform standards.

Threat Assessment and Crime Analysis

The threat assessment section's major component is a review of historical crime data or an in-depth crime analysis. The crime analysis includes spatial and temporal trends, average and mean crime levels, descriptions of the specific types of crime that have occurred, crime totals, violent crime rates, and forecasts or mathematical projections of future crime. The threat assessment may also include a discussion of crime problems in the area and other known threats to the facility.

Vulnerability Assessment

The vulnerability assessment section of the risk assessment report outlines the results of the security survey and identifies any opportunities for adversaries to attack. Weaknesses and deficiencies in the security program should be described in sufficient detail to assist in identifying and selecting effective countermeasures.

Risk Assessment and Recommendations

This section is the pinnacle of the risk assessment report, representing the culmination of a lengthy, comprehensive process. The beginning of this section presents a discussion of the current risks to the facility and to its assets based on the threats and vulnerabilities previously identified during the respective assessments. These risks may be described quantitatively and/or qualitatively. Recommendations developed by the risk assessment teams are then included along with the cost-benefit analysis for each security measure or security mix. Anticipated risk levels after the deployment of the initial or only phase of security measures are then described. Subsequent security deployment phases are then discussed along with further risk reductions expected. The recommendations should be prioritized based on quantitative or qualitative risk ratings for each asset.

Appendices

Appendices should be included in the risk assessment report and should specifically include asset listings and descriptions; existing security inventory documentation; facility and area photographs, blueprints, site diagrams and floor plans; threat assessment and crime analysis information; the security survey instrument or checklist; and cost-benefit worksheets.

Risk Assessment Report Outline

I. Table of Contents
II. Executive Summary
III. Background and Methodology
  A. Risk Assessment Methodology
  B. Assessment Scope and Objectives
  C. Team Composition and Qualifications
  D. Facility Characterization
IV. Assets
  A. Major Assets and Functions
  B. Critical Assets and Functions
V. Existing Security Inventory
  A. Policies and Procedures
  B. Physical Security Measures
  C. Security Personnel
VI. Threat Assessment
  A. Site-Specific Crime Analysis
  B. Historical Attacks against Similar Facilities
VII. Vulnerability Assessment
  A. Security Survey Process
  B. Major Vulnerabilities
  C. Other Vulnerabilities
VIII. Risk Assessment
  A. Current Risks
  B. Risk Ratings
  C. Mitigation Strategies
  D. Prioritized Recommendations
  E. Cost-Benefit Analysis
  F. Revised Risk Estimates
  G. Call for Action
IX. Appendices
  A. Facility and Area Photographs
  B. Blueprints, Site Diagrams, and Floor Plans
  C. Facility Personnel Interview Questions
  D. Complete Asset List and Descriptions
  E. Existing Security Inventory
  F. Threat Assessment and Crime Analysis Documentation
  G. Security Survey Instrument or Checklist
  H. Cost-Benefit Analysis Worksheets

Appendix

ASIS International General Security Risk Assessment Guideline—Qualitative and Quantitative Risk Assessments

ASIS General Security Risk Assessment Guidelines

The following examples of quantitative and qualitative risk assessment approaches are from the General Security Risk Assessment Guideline, Copyright (c) 2003 by ASIS International. Used by permission. The complete guideline is available from ASIS International, 1625 Prince Street, Alexandria, Virginia 22314 or at http://www.asisonline.org/guidelines/guidelines.htm.

Appendix I

Qualitative Approach

Each step of the following seven-step practice advisory includes examples and other relevant information to guide the practitioner in developing a better understanding of the underlying principles to be applied in the assessment.

PRACTICE ADVISORY #1
Understand the organization and identify the people and assets at risk.

COMMENTARY—"Understand the organization."

The first task of the security practitioner is to develop an understanding of the organization to be assessed. This does not mean that the practitioner must become an expert in the operation of the enterprise to be evaluated, but must acquire enough of an understanding of how the organization operates to appreciate its complexities and nuances. Consideration should be given to factors such as hours of operation; types of clients served; nature of the business activity; types of services provided or products produced, manufactured, stored, or otherwise supplied; the competitive nature of the industry; the sensitivity of information; the corporate culture; the perception of risk tolerance; and so on.

The types of information that the practitioner should ascertain are as follows.

- The hours of operation for each department
- Staffing levels during each shift
- Type of services provided and/or goods produced, stored, manufactured, etc.
- Type of clientele served (e.g., wealthy, children, foreigners, etc.)
- The competitive nature of the enterprise
- Any special issues raised by the manufacturing process (e.g., environmental waste, disposal of defective goods, etc.)
- Type of labor (e.g., labor union, unskilled, use of temporary workers, use of immigrants, etc.)

COMMENTARY—"Identify the people and assets at risk."

The second step in the process is to identify the assets of the organization that are at risk to a variety of hazards.

People

People include employees, customers, visitors, vendors, patients, guests, passengers, tenants, contract employees, and any other persons who are lawfully present on the property being assessed. In very limited circumstances, people who are considered trespassers also may be at risk for open and obvious hazards on a property or where an attractive nuisance exists (e.g., abandoned warehouse, vacant building, a "cut through" or path routinely used by people to pass across property as a short cut). In most states, trespassers need only be warned by the posting of signs of a known dangerous or hazardous condition.

Property

Property includes real estate, land and buildings, facilities; tangible property such as cash, precious metals, and stones; dangerous instruments (e.g., explosive materials, weapons, etc.); high-theft items (e.g., drugs, securities, cash, etc.); as well as almost anything that can be stolen, damaged, or otherwise adversely affected by a risk event.

Property also includes the "goodwill" or reputation of an enterprise that could be harmed by a loss risk event. For example, the ability of an enterprise to attract customers could be adversely affected by a reputation as being unsafe or crime ridden.

The third subset of property is information. Information includes proprietary data, such as trade secrets, marketing plans, business expansion plans, plant closings, confidential personal information about employees, customer lists, and other data that if stolen, altered, or destroyed could cause harm to the organization.

PRACTICE ADVISORY #2
Specify loss risk events/vulnerabilities.

COMMENTARY

The second major step in the security risk assessment methodology is to identify the types of events or incidents which could occur at a site based on the history of previous events/incidents at that site; events at similarly situated sites; the occurrence of events (e.g., crimes) that may be common to that type of business; natural disasters peculiar to a certain geographical location; or other circumstances, recent developments, or trends.

Loss risk events can fall into three distinct categories: crimes, noncriminal events such as human-made or natural disasters, and consequential events caused by an enterprise's relationship with another organization, when the latter organization's poor or negative reputation adversely affects the enterprise.

SOURCES OF DATA AND INFORMATION

Crime-Related Events

There are numerous sources for information/data about crime-related events that may impact an enterprise. The security practitioner may consider any of the following sources in aiding the determination of risk at a given location.

- Local police crime statistics and calls for service at the site and the immediate vicinity for a three-to-five-year period
- Uniform Crime Reports published by the U.S. Department of Justice for the municipality
- The enterprise's internal records of prior reported criminal activity
- Demographic/social condition data providing information about economic conditions, population densities, transience of the population, unemployment rates, etc.
- Prior criminal and civil complaints brought against the enterprise
- Intelligence from local, state, or federal law enforcement agencies regarding threats or conditions that may affect the enterprise
- Professional groups and associations that share data and other information about industry-specific problems or trends in criminal activity
- Other environmental factors such as climate, site accessibility, and presence of "crime magnets"

Non-Criminal Events

The practitioners should consider two subcategories of non-crime-related events: natural and "human-made" disasters. Natural disasters are events such as hurricanes, tornadoes, major storms, earthquakes, tidal waves, lightning strikes, and fires caused by natural disasters. "Human-made" disasters or events could include labor strikes, airplane crashes, vessel collisions, nuclear power plant leaks, terrorist acts (which also may be criminal-related events), electrical power failures, and depletion of essential resources.

Consequential Events

A "consequential" event is one where, through a relationship between events or between an enterprise and another organization, the enterprise suffers some type of loss as a consequence of that event or affiliation, or when the event or the activities of one organization damage the reputation of the other. For example, if one organization engages in illegal activity or produces a harmful product, the so-called innocent enterprise may find its reputation tainted by virtue of the affiliation alone, without any separate wrongdoing on the part of the latter organization.

PRACTICE ADVISORY #3

Establish the probability of loss risk and frequency of events.

COMMENTARY—Probability of Loss Risk

Probability of loss is not based upon mathematical certainty; it is consideration of the likelihood that a loss risk event may occur in the future, based upon historical data at the site, the history of like events at similar enterprises, the nature of the neighborhood, immediate vicinity, overall geographical location, political and social conditions, and changes in the economy, as well as other factors that may affect probability.

For example, an enterprise located in a flood zone or coastal area may have a higher probability for flooding and hurricanes than an enterprise located inland and away from water. Even if a flood or hurricane has not occurred previously, the risks are higher when the location lends itself to the potential for this type of a loss risk event.

In another example, a business that has a history of criminal activity both at and around its property will likely have a greater probability of future crime if no steps are taken to improve security measures and all other factors remain relatively constant (e.g., economic, social, political issues).

The degree of probability will affect the decision-making process in determining the appropriate solution to be applied to the potential exposure.

COMMENTARY—Frequency of Events

When looked at from the "event" perspective, the practitioner may want to query how often an exposure exists per event type. For example, if the event is robbery of customers in the parking lot, then the relevant inquiry may be how often customers are in the lot and for how long when walking to and from their vehicles. If the event is the rape of a resident in an apartment building, then the inquiry may focus on how often the vulnerable population is at risk. If the event were a natural disaster such as a hurricane, the practitioner certainly would want to know when hurricane season takes place.

PRACTICE ADVISORY #4
Determine the impact of the event.

COMMENTARY
The security practitioner should consider all the potential costs, direct and indirect, financial, psychological, and other hidden or less obvious ways in which a loss risk event impacts an enterprise. Even if the probability of loss is low, but the impact costs are high, security solutions still are necessary to manage the risk.

Direct costs may include:

- Financial losses associated with the event, such as the value of goods lost or stolen
- Increased insurance premiums for several years after a major loss
- Deductible expenses on insurance coverage
- Lost business from an immediate post-risk event (e.g., stolen goods cannot be sold to consumers)
- Labor expenses incurred as a result of the event (e.g., increase in security coverage post-event)
- Management time dealing with the disaster/event (e.g., dealing with the media)
- Punitive damages awards not covered by ordinary insurance

Indirect costs may include:

- Negative media coverage
- Long-term negative consumer perception (e.g., that a certain business location is unsafe)
- Additional public relations costs to overcome poor image problems
- Lack of insurance coverage due to a higher risk category
- Higher wages needed to attract future employees because of negative perceptions about the enterprise
- Shareholder derivative suits for mismanagement
- Poor employee morale, leading to work stoppages, higher turnover, etc.

PRACTICE ADVISORY #5
Develop options to mitigate risks.

COMMENTARY
The security practitioner will have a range of options available, at least in theory, to address the types of loss risk events faced by an enterprise. "In theory" alludes to the fact that some options may not be available either because they are not feasible (discussed in Practice Advisory #6) or are too costly, financially or otherwise.

Options include security measures available to reduce the risk of the event. Equipment or hardware, policies and procedures, management practices, and staffing are the general categories of security-related options. However, there are other options, including transferring the financial risk of loss through insurance coverage or contract terms (e.g., indemnification clauses in security services contracts), or simply accepting the risk as a cost of doing business.

Any strategy or option chosen still must be evaluated in terms of availability, affordability, and feasibility of application to the enterprise's operation.

PRACTICE ADVISORY #6
Study the feasibility of implementation of options.

COMMENTARY
The practical considerations of each option or strategy should be taken into account at this stage of the security risk assessment. While financial cost is often a factor, one of the more common considerations is whether the strategy will interfere substantially with the operation of the enterprise. For example, retail stores suffer varying degrees of loss from the shoplifting of goods. One possible "strategy" could be to close the store and keep out the shoplifters. In this simple example, such a solution is not feasible because the store also would be keeping out legitimate customers and would go out of business.

In a less obvious example, an enterprise that is open to the public increases its access control policies and procedures so severely that a negative environment is created by effectively discouraging people from going to that facility as potential customers and hence, it loses business.

The challenge for the security practitioner is to find that balance between a sound security strategy and consideration of the operational needs of the enterprise, as well as the psychological impact on the people affected by the security program.

PRACTICE ADVISORY #7
Perform a cost/benefit analysis.

COMMENTARY
The final step in conducting a security risk analysis is consideration of the cost versus benefit of a given security strategy. The security practitioner should determine what the actual costs are of the implementation of a program and weigh those costs against the impact of the loss, financially or otherwise. For example, it would make no sense to spend $100,000 on security equipment to prevent the theft of a $1,000 item, especially when it may make more sense to purchase insurance or remove the item to a more secure location.

Appendix II

Quantitative Approach

CALCULATING PROBABILITY AND CRITICALITY

LOSS EVENT PROFILE

Forecasting individual loss events that may occur is the first step in dealing with risk assessment. It requires clear ideas about the kinds of loss events or risks, as well as about the conditions, circumstances, objects, activities, and relationships that can produce them. A security countermeasure can be planned if the loss event has the following characteristics:

- The event will produce an actual loss, measurable in some standard medium, such as money; and
- The loss is not the result of a speculative risk in that nonoccurrence of the event would not result in a gain.

The kinds of events that are loss-only oriented and which involve so called pure risks include crime, natural catastrophe, industrial disaster, civil disturbance, war or insurrection, terrorism, accident, conflicts of interest, and maliciously willful or negligent personal conduct. The recognition of even obvious risks implies some estimate of the probability that the risk actually will produce a loss. To the extent that the risk itself is concealed, the task of estimating probability of occurrence is more difficult.

LOSS EVENT PROBABILITY OR FREQUENCY

Probability can be formulated as the number of ways in which a particular event can result from a large number of experiments which could produce that event, divided by the number of those experiments. Stated as an equation, this is:

$$P = \frac{f}{n}$$

where:

P = the probability that a given event will occur
f = the number of actual occurrences of that event
n = the total number of experiments seeking that event

E.g., the probability of shoplifting at a given location during a given year is determined as: *P* (probability) = the number of days on which actual shoplifting events occurred during the year divided by 365. Although this simple statement illustrates a direct way to calculate probability mathematically, it is not enough for practical application to security loss situations, because while some events will occur more than once, other events will occur only once, and the reaction will so change the environment that the theoretically probable further occurrences will be prevented. As a basic concept, *the more ways a particular event can occur in given circumstances, the greater the probability that it will occur.* For effective assessment of probability, as many as possible of those circumstances that could produce the loss must be known and recognized.

Probability Factors

Conditions and sets of conditions that will worsen or increase asset exposure to risk of loss can be divided into the following major categories:

1. *Physical environment* (construction, location, composition, configuration)
2. *Social environment* (demographics, population dynamics)
3. *Political environment* (type and stability of government, local law enforcement resources
4. *Historical experience* (type and frequency of prior loss events)
5. *Procedures and processes* (how the asset is used, stored, secured)
6. *Criminal state-of-the-art* (type and effectiveness of tools of aggression)

Application of Probability Factors Analyses

The practical value of loss risk analysis depends upon the skill and thoroughness with which the basic risks to an enterprise are identified. This is the first and most important step in the entire process. Every aspect of the enterprise or facility under review must be examined to isolate those conditions, activities, and relationships that can produce a loss. For an effective analysis, the observer must take into account the dynamic nature of the enterprise on each shift and between daylight and darkness. The daily routine must be understood because the loss-producing causes can vary from hour to hour.

Checklists

Every enterprise differs from every other, and general recommendations must be modified to meet local needs. Consult the references in this guideline for forms and checklists to use in the initial gathering of loss event data.

RISK MATRIX

After analysis has identified the specific threats or risks, the details that make occurrence of each event more or less probable can be recorded. The method suggested is a grid or matrix arranged either by asset or by type of risk, setting forth all the factual elements relevant to probability. Matrices describe a particular situation with respect to each of the risks identified in the general fact gathering. Please see Figure 1, infra. The frequent absence or scarcity of historical occurrence data often makes it impossible to calculate probability on a purely quantitative basis and requires some degree of qualitative assessment.

Asset Identification and Description

		CONDITIONS AFFECTING RISK				
LOCATION	**Value ($)**	**Admittance Controlled (Y/N)**	**Area Locked (Y/N)**	**Records Kept (Y/N)**	**Alarms (Y/N)**	**Other**
Warehouse						Etc.
Front Office						Etc.
Laboratory						Etc.
Shipping						Etc.
Manufacturing						Etc.
Etc.						Etc.

Figure 1. Specimen Matrix. Locations and Conditions Affecting Risk Can Be Added and/or Modified to Fit the Particular Asset and Its Environment. (Y/N) = Yes or No for Each Condition Specified. Conditions Should Be Framed Such That a Yes Indicates Better and a No Indicates Poorer Protection.

Probability Ratings

After all the available data concerning each risk and its factual circumstances have been gathered, a probability rating can be assigned to that risk. Ratings will not consider any precaution or countermeasure that may later be taken to reduce or eliminate the risk. A primary purpose of such unconditioned ratings is to allow for later priority scheduling in the selection of countermeasures. It may be enough to be able to say that one event is more probable than another. To say this about entire series or categories of events, it must be possible to assign each to some class that can then be compared with other classes to arrive at a conclusion of "more likely" or "less likely." Five categories of probability can establish useful distinctions among events, as follows:

(A) Virtually Certain — Given no changes, the event will occur. For example, given no changes, a closed intake valve on a sprinkler riser will prevent water flow in the event of fire.

(B) Highly Probable — The likelihood of occurrence is much greater than that of nonoccurrence. For example, unprotected currency lying visible on a counter is very likely to be taken.

(C) Moderately Probable — The event is more likely to occur than not to occur.

(D) Less Probable — The event is less likely to occur than not to occur. This does not imply impossibility, merely improbability.

(E) Probability Unknown — Insufficient data are available for an evaluation.

This approximate system of ratings contains wide latitude for variation. Two observers could assign different probabilities to the same risk, based upon different evaluations of the circumstances. But an advantage of this technique is that absolute precision is not important. If the correct general label can be attached, it does not matter that a highly probable risk might have a ratio of .751 or .853. What is important is to be able to segregate all risks of virtually certain probability from all others and to make similar distinctions for each other general class. Even competent professionals may disagree on what is highly probable and what is moderately probable. To compensate for inexactness, if a rating is in doubt after all available information has been gathered and evaluated, then the higher of two possible ratings should be assigned.

Rating Symbols. To save time and space, five levels of probability can be assigned the symbols **A, B, C, D,** and **E,** ranking downward from "Virtually Certain" to "Probability Unknown." These symbols later will be combined with symbols representing criticality in the development of priority lists. It should be noted that the probability rating **E,** or "Probability Unknown," is merely a temporary rating pending the development of all relevant data. In the construction of threat logic patterns, **E** ratings will be replaced by one of the definite ratings.

The second step in risk analysis is complete when a particular risk, identified in the first level of the survey through the use of forms and checklists, has been assigned a probability rating. No standard recording system is in universal use, and each protection organization making a survey must set up its own recording system to be sure that each risk, once identified, can be found readily again in the growing volume of survey data. A simple method for doing this is to assign a distinctive number to each risk classified. It will be necessary to locate and identify each risk to add a later criticality rating, to rank the rated risk in a table or priority list, and to plot it in a threat logic tree based on relative priorities.

LOSS EVENT CRITICALITY

Highly probable risks may not require countermeasures attention if the net damage they would produce is small. But even moderately probable risks require attention if the size of the loss they could produce is great. The correlative of probability of occurrence is severity or criticality of occurrence. Assessing criticality is the third step in risk assessment. Criticality is first considered on a single event or occurrence basis. For events with established frequency or high-recurrence probability, criticality also must be considered cumulatively. The criticality or loss impact can be measured in a variety of ways. One is effect on employee morale; another is effect on community relations. But the most useful measure overall is financial cost. Because the money measure is common to all ventures, even government and not-for-profit enterprises, the seriousness of security vulnerability can be grasped most easily if stated in monetary terms.

Note that some losses (e.g., loss of human life, loss of national infrastructure elements, or losses of community goodwill) do not lend themselves to ready analysis in financial terms. When events that could produce these types of losses have been identified, some factors other than merely quantitative will be used to measure their seriousness.

When tradeoff decisions are being made as part of the risk management process, a very useful way to evaluate security countermeasures is to compare cost of estimated losses with cost of protection. Money is the necessary medium.

Kinds of Costs to Be Considered

Costs of security losses are both direct and indirect; they are measured in terms of lost assets and lost income. Frequently, a single loss will result in both kinds.

1. Permanent Replacement

The most obvious cost is that involved in the permanent replacement of a lost asset. Permanent replacement of a lost asset includes all of the cost to return it to its former location. Components of that cost are (1) *Purchase price* or *manufacturing cost*; (2) *Freight and shipping charges*; and (3) *Make-ready or preparation cost to install it or make it functional.* A lost asset may cost more or less to replace now than when it was first acquired.

2. Temporary Substitute

It may be necessary to procure substitutes while awaiting permanent replacements. This may be necessary to minimize lost opportunities and to avoid penalties and forfeitures. The cost of the temporary substitute is properly allocable to the security event that caused the loss of the asset. Components of temporary substitute cost might be (1) *Lease or rental*; and/or (2) *Premium labor*, such as overtime or extra shift work to compensate for the missing production.

3. Related or Consequent Cost

If other personnel or equipment are idle or underutilized because of the absence of an asset lost through a security incident, the cost of the downtime also is attributable to the loss event.

4. Lost Income Cost

In most private enterprises, cash reserves are held to the minimum necessary for short-term operations. Remaining capital or surplus is invested in varying kinds of income-producing securities. If cash that might otherwise be so invested must be used to procure permanent replacements or temporary substitutes or to pay consequent costs, the income that might have been earned must be considered part of the loss. If income from investment is not relevant to a given case, then alternative uses of the cash might have to be abandoned to meet the emergency needs. In either case, use of the money for loss replacement will represent an additional cost margin. To measure total loss impact accurately, this also must be included. The following formula can be used:

$$I = \frac{P \times r \times t}{365}$$

where:

I = income earned
P = principal amount (in dollars) available for investment
r = annual percent rate of return
t = time (in days) during which P is available for investment

Cost Abatement

Many losses are covered, at least in part, by insurance or indemnity of some kind. To the extent it is available, that amount should be subtracted from the combined costs of loss enumerated previously.

A Cost-of-Loss Formula

Taking the worst-case position and analyzing each security loss risk in light of the probable maximum loss for a single occurrence of the risk event, the following equation can be used to state that cost:

$$K = Cp + Ct + Cr + Ci - I$$

where:

K = criticality, total cost of loss
Cp = cost of permanent replacement
Ct = cost of temporary substitute
Cr = total related costs
Ci = lost income cost
I = available insurance or indemnity

Criticality Ratings

It is suggested that the following ratings be used to summarize the impact of each loss event, and interpreted as follows:

1. **Fatal** — The loss would result in total recapitalization or abandonment or long-term discontinuance of the enterprise.
2. **Very serious** — The loss would require a major change in investment policy and would have a major impact on the balance sheet assets.
3. **Moderately serious** — The loss would have a noticeable impact on earnings as reflected in the operating statement and would require attention from the senior executive management.
4. **Relatively unimportant** — The loss would be charged to normal operating expenses for the period in which sustained.
5. **Seriousness unknown** — Before priorities are established, this provisional rating is to be replaced by a firm rating from one of the first four classes.

The nature and size of the enterprise determines the dollar limits for each of these classes. The value of the rating system is in its relevance to the enterprise. The terms used are not intended to have any absolute significance. This completes the third step in vulnerability assessment.

ALTERNATIVE APPROACHES TO CRITICALITY

Known Frequency Rate

There are other ways in which the weighted importance of a probable risk event can be measured. One is when a historical frequency can be identified. For example, natural catastrophes such as floods and earthquakes are expected to occur a stated number of times per year, based on the number of actual past occurrences. Other events also may have a reliable rate of recurrence. When a frequency rate is known, the single-event criticality can be multiplied by the number of events expected during the period considered, normally the calendar or fiscal year. Thus, if K = \$10,000 for an event, and it has a frequency rate of once a year, the weighted impact would be \$10,000 × 1. If the same event had a frequency rate of once every three years, the weighted impact would be \$10,000 × .333 or \$3,333. If it had a frequency of three times a year, the weighted impact would be \$10,000 × 3 or \$30,000.

Nominal Numerical Probability

Another technique, useful to convert the symbolic rankings to simple numerical statements, is to assign an agreed real numerical probability to each of four categories below. Thus: A) "Virtually Certain," might be assigned a numerical probability of .85; B) "Highly Probable" might be assigned .65; C) "Moderately Probable" might be assigned .50; and D) "Less Probable" might be assigned .20.

Next, the criticality of any single loss event is multiplied by the agreed value of the probability. Thus, a \$10,000 criticality for a moderately probable event would be \$10,000 × .50 = \$5,000. (Note that this is used hypothetically to arrive at an overall picture of exposure. If the loss occurs at all, it will cost \$10,000, not \$5,000.) But to permit ranking before loss so as to expedite countermeasures, the technique would preserve the weighted differences.

Scatter Plots

Another method that can be used to present overall risk is to use a scatter plot. This is a method of plotting each risk on a graph whose axes are cost and frequency. First, the criticality or cost impact is located on the vertical axis. Then, moving right in a straight line, a dot or mark is placed above the frequency rate for that event on the horizontal axis. When all the risks have been plotted on the graph, a smooth curve (a line passing through the areas of highest concentration of dots) can be drawn. This would indicate the approximate distribution of expected losses for the planning period. The countermeasures program would be designed to lower that line as much as feasible. See Figure 2, infra.

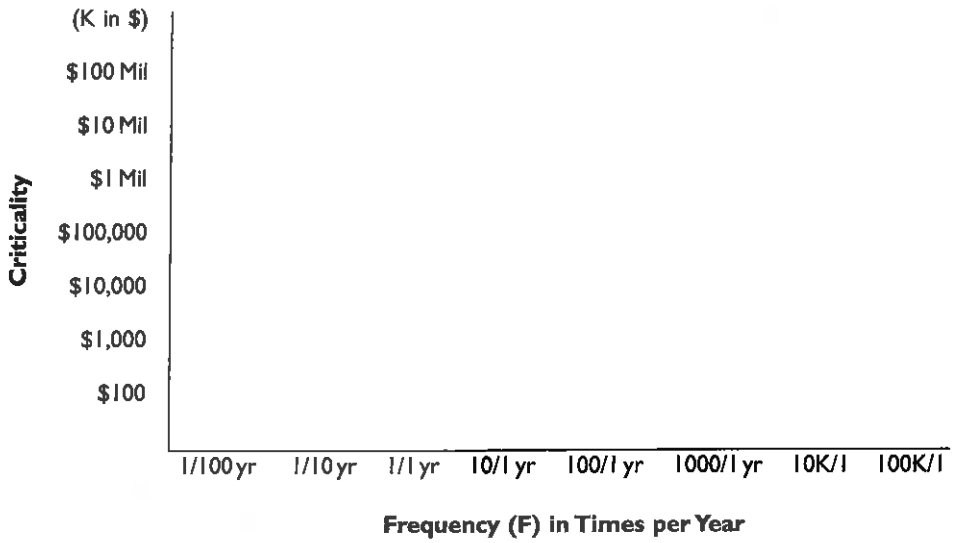

Figure 2. Specimen Scatter Plot; to Show Events Weighted for Criticality (K) (Vertical Axis) and Frequency (Times per Year) (Horizontal Axis). Each Event or Risk Is Plotted at the Intersection of K and F for that Event.

Establishing Priorities

The next step is to arrange the entire body of rated risks into a sequence of priority for countermeasures attention. The more serious risks are listed first, followed in descending order of importance by the others until all the risks have been listed. The listing should identify each risk and indicate the combined probability criticality rating that has been assigned. Such an approach would produce a list of all the risks in each of the various rating classes, as follows: A1, A2, A3, A4; B1, B2, B3, B4; C1, C2, C3, C4; D1, D2, D3, D4.

When all the risks have been ranked, the formal task of risk assessment is complete and reflects the risk exposure of the enterprise as of the date on which the assessment was made. No risk assessment is permanent and, depending upon the extent and speed of changes within the enterprise, reassessments will be required periodically, at a minimum of at least once a year.