Chapter 1

Security Risk Assessment and Management Process

1.1 INTRODUCTION

Since September 11, 2001, decisions for security risk managers have become even more difficult. The terrorist threat potential, that is, the likelihood of an attack, motivations, and capabilities, has dramatically increased. The need to add security features has placed a heavy burden on the already strained budgets of government and commercial enterprises. Some companies have had to decide whether or not they can maintain their business and provide the required security to adequately protect their facilities and the lives of their employees. Security risk managers need a mechanism to help them analyze the information that they do have to make the most logical business decisions to protect their facilities against the very real potential of malevolent acts.

First, managers must define what is essential to the mission of the facility: What are the undesired security events that would interrupt the mission, the consequences associated with the events, the targets that must be protected to prevent the security events, and the liabilities incurred? Concurrent with determining what is important to the mission is identifying what to protect against, that is, defining the adversarial threat spectrum to understand who might attempt the undesired event(s). The adversarial threat spectrum could include international or domestic terrorists, religious or political extremists, criminals, the mentally deranged, or the insider employee. Next, a system effectiveness analysis or vulnerability analysis is completed to determine how well the current security system protects against the adversarial threat spectrum for the undesired events. Once the security system's effectiveness is known, the security risk can be estimated and the manager must assess whether or not the risk level is acceptable. If the risk level is deemed to be too high, the manager must consider the impacts on operations and costs to reduce risk by improving the security system or reducing the consequences. Balancing the resultant impacts and risk reduction can present quite a challenge, but is of utmost importance. (See Figure 1.1.)

This chapter will outline a validated risk assessment and management process that supports managers in determining how much security is enough for their facility, business, or industry. Each following chapter in this book will support one or more steps of the Security Risk Assessment and Management Process. The process can be and has been adapted for various applications, including many elements of our nation's critical infrastructure.

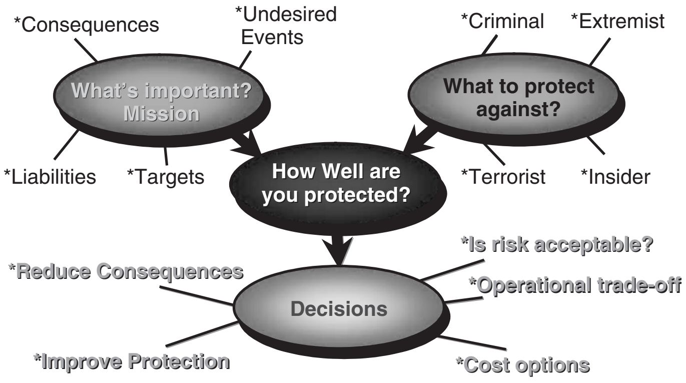


Figure 1.1 Decisions for Security Risk Managers.

The risk assessment and management process was developed at Sandia National Laboratories (SNL) in the 1990s for the Interagency Forum for Infrastructure Protection (IFIP). The IFIP was formed when various related government agencies with common security concerns came together to address security protection against the terrorist threat, as called for by Presidential Decision Directive #63, signed by former President Bill Clinton. Proven physical protection tools and concepts resulting from thirty years of testing and development at SNL were integrated into a single methodology for assessing infrastructure and life-threatening risk. The process was originally applied to the protection of federal dams, high-voltage electric power transmission systems, and other critical national infrastructures. The tool was completed, tested, and published a month before 9/11, and has since been used to estimate relative security risk level and to assess the protection effectiveness and design security and consequence mitigation systems of hundreds of government and commercial facilities against malevolent acts.

However, security risk is difficult to quantify. The traditional risk equation can be used to begin the process. Traditionally, security risk is a function of the likelihood of adversary attack, the likelihood that the adversary attack is successful, and the consequences associated with the loss to the attack. The relative risk estimation process described here is qualitative in nature and allows decision makers to rank events in relative order, to enable them to make risk management decisions. Figure 1.2 describes the three parameters used to estimate security risk.

The conclusions drawn and the information used in the application of the risk assessment process produce sensitive company information that must be protected. The level of protection of the information and the means of protection must be determined, planned, and implemented before the analysis begins. The three factors of the security risk equation each encompass

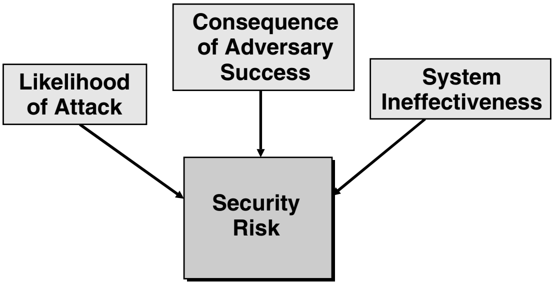


Figure 1.2 Parameters Used to Estimate Security Risk.

information that, if compromised, could provide serious advantage to the adversary.

1.2 SECURITY RISK EQUATION

Security risk is estimated by the following traditional risk equation:

$$R = P_A * (1 - P_E) * C$$

where:

$$\begin{aligned} R &= \text{risk associated with adversary attack} \\ P_A &= \text{likelihood of attack} \\ P_E &= \text{probability that the security} \\ &\quad\ \text{system is effective against the attack} \\ (1 - P_E) &= \text{system ineffectiveness} \\ C &= \text{consequence of the loss from the attack} \end{aligned}$$

Security risk is difficult to quantify, because the basic assumptions for calculating mathematical probability cannot be met; that is, the variables are neither independent nor random. Estimating the likelihood that an adversary will decide to attack a given facility is difficult, at best, because predicting human behavior can never be a random event in the mathematical sense. Humans continually plan, practice, learn, and modify their behaviors. For these reasons, quite often analysts will estimate conditional risk for security applications. Conditional risk presumes that the initiating event occurs (for security applications, this means that the adversary does decide to attack and conducts the attack against the specific facility).

This assumption can focus the risk assessment on the likelihood of adversary success and the associated consequences resulting from the attack. Sometimes building owners and operators need more concrete resolution in risk estimates. They may have several buildings that are vulnerable to the threat, and the consequence of loss is high, but they have credible evidence that makes them believe that one building is more or less likely to be attacked than another, and they feel they must prioritize their security spending, especially if funds are limited.

Various risk assessment and risk management methods have been developed. While each method has its own unique name, focus, and methodology, all attempt to answer three fundamental questions:

1. What are the bad things that can happen to my facility?
2. How likely are the bad things?
3. How do they affect my facility – its mission, occupants, surroundings, and the larger environment?

This text will provide a process to estimate relative security risk based on qualitative estimates for three risk parameters:

- **Likelihood of attack** – Qualitative estimate for likelihood of adversary attack, P_A. Note that threat potential for attack, likelihood of attack, and P_A mean the same thing in this text.
- **Consequence of successful adversary attack** – Qualitative estimate of consequence, C.

- **System ineffectiveness (1 – $\mathbf{P_E}$)** – Qualitative estimate of adversary success or the complement of system effectiveness, P_E.

1.3 SECURITY RISK ASSESSMENT AND MANAGEMENT PROCESS

An analytic process is used to assess security risk. Figure 1.3 describes the order and sequence of the basic steps of the process. The process begins with an optional screening analysis for corporations to prioritize their facilities, followed by characterization of the subject facility, including identification of the undesired events and the respective critical assets. Guidance for defining an adversarial threat is included, as well as for using the definition of the threat to estimate the threat potential for attack or likelihood of adversary attack at a specific facility. Relative values of consequence are estimated. Another optional step allows the owner to prioritize the

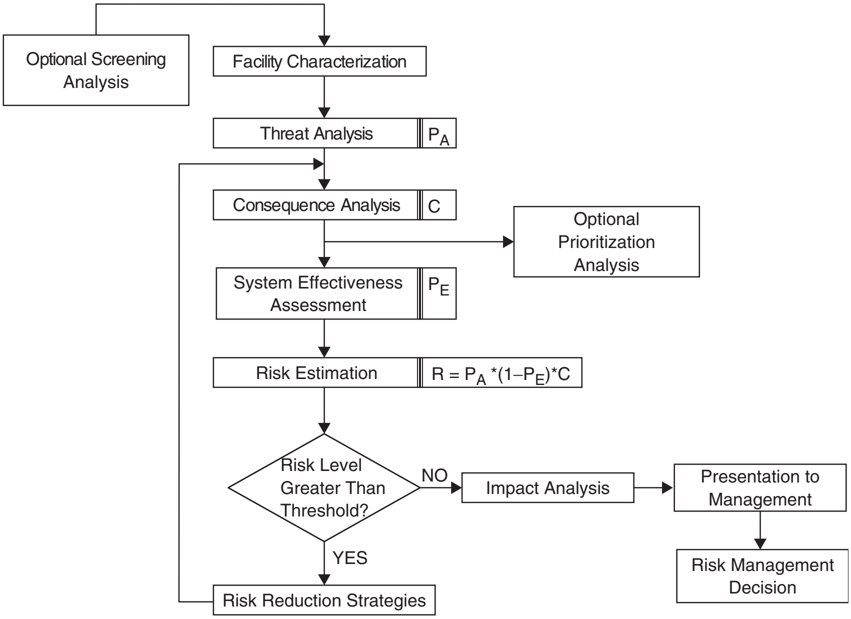

Optional Screening Analysis
Facility Characterization
Threat Analysis
P_A
Consequence Analysis
C
Optional Prioritization Analysis
System Effectiveness Assessment
P_E
Risk Estimation
$R = P_A*(1-P_E)*C$
Risk Level Greater Than Threshold?
NO
Impact Analysis
Presentation to Management
YES
Risk Management Decision
Risk Reduction Strategies

Figure 1.3 Security Risk Assessment and Management Process.

assets at a given facility. Methods are also included for estimating the effectiveness of the security system against the adversary attack. Finally, relative risk is estimated. In the event that the value of risk is deemed to be above a predetermined threshold (too *High*), the methodology addresses a process for identifying and evaluating risk reduction strategies in order to reduce risk.

1.3.1 Facility Characterization

An initial step in security system analysis is to characterize the facility to be analyzed. Facility characterization requires a thorough understanding of the mission and operating conditions of the building, as well as the security concerns. The security concerns should describe the undesired events – the specific events that, ideally, the protection system should prevent. An extension of describing the undesired events is identification of the company's critical assets that an adversary would most likely be attempting to harm or obtain. Sometimes the assets to be protected are obvious by inspection; in complex operations, an analytical logic approach may be required to ensure that all of the critical assets are identified and protected.

Facility characterization includes a complete physical description, not only of the physical layout of the building but also of the construction details, locations of site boundaries, building locations, floor plans, and access points as well as policy and procedures and physical and cyber-protection features and their locations. Any known vulnerabilities or weaknesses in protection are noted.

The facility characterization concludes with a statement of the protection objectives for the facility. Usually, the protection objectives are a list of undesired events or some subset of the undesired events and a listing of the respective critical asset(s) to be protected. For example, a protection objective of a building might be to ensure health and safety for building occupants or to prevent the theft of a particular critical asset.

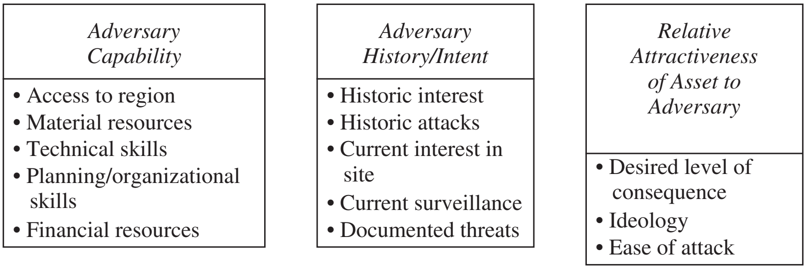
1.3.2 Threat Analysis

The first parameter of the risk analysis process is the threat potential, particularly, the likelihood of adversary attack.

Threat – Before a vulnerability analysis can be completed and before threat potential for attack or likelihood of attack can be estimated, a description of the threat is required. This description includes the types of possible adversaries, tactics, and capabilities (e.g., number in the group, weapons, equipment, and transportation mode). The threat definition is often reduced to several paragraphs that describe the type and number of adversaries, their modus operandi, the type of tools and weapons they would use, and the type of events or acts they are willing to commit.

The types of organizations that may be contacted during the development of a threat definition include local, state, and federal law enforcement and related intelligence agencies. Local authorities should be able to provide reports on the types of criminal activities occurring and analytical projections of future activities. A review of literature may also be conducted to include past incident reports associated with the site, local periodicals, professional journals, and other related material.

Threat Potential for Attack (Likelihood of Attack) – After the adversarial threat spectrum has been described, the information can be used together with statistics of past events and site-specific perceptions to categorize threats in terms of likelihood that each type of threat would attempt an undesired event. Ideally, the model for security risk assessments could be similar to the model for safety risk assessments; the likelihood of an initiating (abnormal) event is estimated and combined with the likelihood of consequences caused by the initiating event. Safety studies have yielded historical data and statistics that can help predict the likelihood of an abnormal event and the system response to the event. However, estimating the likelihood that an adversary group will



Adversary Capability

- Access to region
- Material resources
- Technical skills
- Planning/organizational skills
- Financial resources

Adversary History/Intent

- Historic interest
- Historic attacks
- Current interest in site
- Current surveillance
- Documented threats

Relative Attractiveness of Asset to Adversary

- Desired level of consequence
- Ideology
- Ease of attack

Figure 1.4 Estimating Threat Potential (Likelihood of Attack) for Attack.

attack a specific asset will always represent a challenge because of the human element.

However, a qualitative relative threat potential parameter can be used to estimate the level of the unquantifiable variable. Estimating the threat potential follows a complete threat analysis, and the parameter is estimated per undesired event and per adversary group. The basis of the parameter estimation is:

- Characteristics of the adversary group relative to the asset to be protected
- Relative attractiveness of the asset to the adversary group

Figure 1.4 includes information that can be used to estimate the likelihood that a given adversary group would decide to attack a specific facility.

1.3.3 Consequence Analysis

The second parameter of security risk is consequence. Consequence analysis can be completed after the undesired events and associated critical assets have been identified as a part of facility characterization. The next analysis step is to estimate consequences associated with the loss of specific critical asset(s) for each undesired event. Consequence definitions are site- or industry-specific. Organizations describe consequence in categories or terms

Table 1.1 Consequence Definitions

Consequence Category	*Consequence Level*
Could result in death, permanent total disability, loss exceeding $1M, or irreversible severe environmental damage that violates law or regulation.	Catastrophic
Could result in permanent partial disability, injuries, or occupational illness that may result in hospitalization of at least three personnel, loss exceeding $200K but less than $1M, or reversible environmental damage causing a violation of law or regulation.	Critical
Could result in injury or occupational illness resulting in one or more lost workday(s), loss exceeding $10K but less than $200K, or mitigatible environmental damage without violation of law or regulation, where restoration activities can be accomplished.	Marginal
Could result in injury or illness not resulting in a lost workday, loss exceeding $2K but less than $10K, or minimal environmental damage not violating law or regulation.	Negligible

that are meaningful to them; some may measure consequence in terms of lost income or downtime, others in casualties or illness, and others in terms of loss of pubic confidence or reputation. The consequence categories, such as dollars, deaths, injuries, downtime duration, and negative publicity, that characterize consequence must be determined first. Further, definitions must be established for qualitative levels for each consequence category. Table 1.1 provides an example of a Consequence Definition Table that is similar to one used by the Department of Defense in accordance with Military Standard 882D. The primary goal of consequence analysis is to estimate the relative consequence value associated with each undesired event due to loss or compromise of a critical asset.

1.3.4 System Effectiveness Assessment

The third parameter in assessing security risk, system ineffectiveness ($1 - P_E$), can be derived from a security system effectiveness assessment. Security system ineffectiveness (adversary success) and security system effectiveness (P_E) are complementary functions. If security system effectiveness is *High*, then security system ineffectiveness (adversary success) is judged to be *Low*. The risk assessment process will evaluate security system effectiveness in order to estimate system ineffectiveness (adversary success). A defensible measure of the effectiveness of the security system to prevent the undesired events for the given threat spectrum is an important factor in the security risk equation.

The process focuses on security system effectiveness assessment. A valuable product of assessing system effectiveness is the identification of specific vulnerabilities of the protection system. If the security system effectiveness is judged to be *Low*, specific weaknesses and the associated deficient protection elements causing the *Low* level are site-specific system vulnerabilities. Knowledge of site-specific vulnerabilities is valuable for planning system upgrades to reduce risk and for contingency planning to know where to place reinforcement protection during times of elevated threat conditions.

For most applications, a security system is made up of physical protection features and cyber-protection features. Some undesired events can be accomplished by a physical attack on the facility, whereas others can be accomplished by a cyber-attack on the system. A total security system should address both physical and cyber-attacks, as appropriate. A complete system effectiveness assessment will include a physical protection analysis and cyber-protection analysis.

1.3.4.1 Physical Protection System Effectiveness

An effective physical protection system (PPS) must be able to detect the adversary early enough and delay the adversary long enough for the security response force to arrive and neutralize the adversary before the mission is accomplished. In particular, an effective PPS provides effective detection, delay, and response. These physical system functions (detection, delay, and response) must be integrated to ensure that the adversarial threat is neutralized before the mission is accomplished.

Detection, the first required sequential function of a PPS, is the discovery of adversary covert or overt actions and includes sensing actions. In order to discover an adversary action, the following events must occur:

- Sensor (equipment or personnel) reacts to an abnormal occurrence and initiates an alarm
- Information from the sensor and assessment subsystems is reported and displayed
- Someone assesses the information and determines the alarm to be valid or invalid

Delay is the second required function of a PPS. Any feature that impedes adversary progress can be considered to be delay. Delay can be accomplished by barriers (e.g., doors, vaults, locks) or by distances that cause a time delay to traverse. The security protective force can be considered an element of delay if personnel are in fixed and well-protected positions.

Response, the third requirement of a PPS, comprises actions taken by the security police force (law enforcement officers) to prevent adversarial success. Response consists of interruption of and neutralization of the adversary action.

1.3.4.2 Cyber-Protection System Effectiveness

Much like an effective PPS that demonstrates high performance for the three functions of detection, delay, response, and the integration of these functions, an effective cyber-protection system demonstrates high performance for three basic cyber-security functions and their integration. These functions are used to ensure the properties of confidentiality, integrity, and availability of data. *Confidentiality* requires that information not be made available to unauthorized individuals, entities, or processes. *Integrity* requires that information not be altered or destroyed in an unauthorized manner. *Availability* requires that information be accessible and usable on demand by an authorized entity. The three cyber-protection functions are:

- Authentication
- Authorization
- Audit

The authentication, authorization, and audit must be performed at a high level and must be integrated. The authentication and authorization strategies both provide data to the audit capability where it is analyzed for evidence of malicious activity.

Authentication – Authentication establishes the validity of a claimed identity. User authentication is the capability of associating a computer identity with a human being. This may be done using mechanisms that fall into three categories: (1) something the individual knows, (2) something the individual has, and/or (3) something the individual is. Once a user is authenticated, he or she is generally issued credentials that are associated with computer processes acting in the user's behalf. User authentication is critical to the overall security of a system or network, because if one user obtains (maliciously or otherwise) another user's credentials, then he or she can access any information that the user is permitted to access.

Authorization – Authorization determines what actions an entity is allowed to perform with respect to a given information object (e.g., files, database records, web pages). Authorization for access to systems and applications must be granted by management. Authorization for access to information on systems must be controlled so that only authorized users can access specified information objects, based upon their authenticated identity.

Audit – Audit records the actions or attempted actions performed by an entity within a computer system or network. The cyber-intrusion detection system supports the audit function. The major components of a successful cyber-intrusion detection system are the continual review of traffic data, scanners that detect any unusual occurrences, including any suspect ports or modems, virus protection, and monitors for access control.

Access control monitoring ensures a complementary relationship between firewalls and intrusion detection systems. Firewalls block undesired network traffic and permit desired traffic. The cyber-intrusion detection system inspects both blocked and permitted traffic for suspect patterns.

1.3.4.3 Security System Performance Assessment

Analysis and evaluation of protection systems begins with a review and thorough understanding of the protection objectives and security environment. Analysis can be performed by simply checking for the required features of an effective protection system, such as intrusion detection, entry control, access delay, response communications, and a response force for a physical system and features for authentication, authorization, and audit for a cyber-protection system. However, a system based on required features usually does not lead to a high-performance system because those features are often not integrated to ensure adequate levels of protection for the identified threat spectrum. Sophisticated analysis and evaluation techniques can be used to estimate the minimum performance levels achieved by a security system. The most reliable effectiveness measure is performance as a total integrated system.

1.3.5 Risk Estimation

Security risk is a function of the likelihood of attack, consequence of successful attack, and security system ineffectiveness. To estimate relative security risk, the qualitative estimates for likelihood of attack, system ineffectiveness, and consequence are logically combined. A simple method, based on expert judgment, for combining the three risk parameters to estimate security risk will be discussed. The security risk estimates are relative, not absolute, but they can be used to make risk management decisions. A relative risk level is valuable to:

- Compare risk levels for a spectrum of malevolent threats
- Compare risk levels for a spectrum of facilities, industries, or organizations
- Compare the cost-effectiveness and other impacts of potential improvements

1.3.6 Comparison of Estimated Risk Levels

Estimated risk levels are compared to a predetermined risk threshold to decide whether further analysis is required. The threshold is determined by the analysis team and the security risk managers.

1.3.7 Risk Reduction Strategies

If the estimated baseline risk level for the threat spectrum is judged to be above the established threshold (too *High*), risk reduction strategies for the system may be considered. Risk reduction strategies focus on reducing the levels of the parameters of the security risk equation: likelihood of attack, system ineffectiveness, and consequence. In practice, risk reduction is made most successful by improving protection system effectiveness and mitigating consequences.

Risk Reduction Upgrades – Security system planners must address how to reduce security risk. Planners might consider adding features to increase physical or cyber-protection system effectiveness and/or to reduce or mitigate consequences. Site-specific vulnerabilities identified in the system effectiveness analysis provide guidance for adding/modifying features. Upgrades to the system might include retrofits, additional safeguard features, or additional consequence mitigation features. Consequence analysis and system effectiveness analysis should then be repeated for the upgraded system in order to estimate a risk level associated with the upgraded system. If the estimated risk for the upgraded system is below the threshold, the upgrade is completed. If the risk is still above the threshold, the upgrade process should be repeated until the risk level is judged to be below the threshold.

Impact Analysis – Once the system upgrade has been determined, it is important to evaluate the impacts of the risk reduction on the mission of the facility and the cost. If system upgrades put a heavy burden on normal operation, a trade-off would have to be considered between risk and operations. Budget can be the driver in implementing security upgrades. A trade-off between risk and total cost may have to be considered. The assessed level of risk and the upgrade impact on cost, mission, and schedule are valuable information to security risk managers.

1.4 PRESENTATION TO MANAGEMENT

The final step in the risk assessment process is the preparation of a presentation package for the risk managers and stakeholders. The presentation generally includes the threat description, the security risk estimates for the baseline system, descriptions of any risk reduction packages, and the results of the impact analysis for the risk reduction package(s). By using comparison to the baseline risk levels, managers are able to understand what the upgrade package is buying them in risk reduction as well as other potential impacts. The total presentation package provides invaluable information for risk management decision makers.

1.5 RISK MANAGEMENT DECISIONS

Building owners, stakeholders, and risk managers have the risk assessment information package to help them make difficult security decisions. Most importantly, risk managers must decide on the design basis threat or the threat level to which the security system will be designed.

1.6 INFORMATION PROTECTION

The risk assessment process provides valuable, detailed information for risk managers; likewise, the information could provide valuable information to any potential adversaries. Because the process begins with basic facts and assumptions and each step builds on previous step(s), allowing the information to get into the wrong hands could provide a roadmap for the malevolent threat. Each step of the process provides security sensitive information:

1. **Facility characterization** identifies the security concerns, critical asset(s), and their locations.
2. **Threat analysis** ultimately defines the level of protection to which the security system is designed. If the perceived highest threat level is the terrorist, the security system will be designed to be much stronger than if the perceived threat is the vandal.
3. **Consequence analysis** prioritizes the assets in terms of criticality or value.
4. **System effectiveness assessment** provides possible attack scenarios and documented system weaknesses or vulnerabilities.

For these reasons, once the process is applied to a specific facility, the entire analysis package must be protected. Most sites will have to develop the infrastructure for protecting, storing, and sharing the risk assessment package.

1.7 PROCESS SUMMARY

This chapter provides an overview of an analytical security risk assessment and management process. Application of the risk assessment process supports managers in determining how much security is enough for their facility, business, or industry. The required steps of the process are:

1. Characterize the facility.
2. Analyze the malevolent threat and estimate the threat potential for attack of the facility.
3. Estimate consequences associated with the attack.
4. Assess the effectiveness of the physical and cyber-protection systems.
5. Estimate relative security risk as a function of likelihood of attack, security system ineffectiveness, and consequence.
6. Compare the security risk level to a predetermined threshold.
7. Suggest risk reduction strategies if the estimated risk level is above threshold, followed by re-evaluating consequences and protection system effectiveness to measure and ensure relative risk reduction.
8. Analyze impacts imposed by risk reduction packages.
9. Present completed assessment to management.
10. Make risk management decisions.

The process begins with basic facts and assumptions, and each step builds on previous step(s). The final results are defendable because they are traceable back to the original facts and assumptions. Results are repeatable, and updates to any step are easily addressed without starting all over. The process can be adapted to assess the security risk for most entities. The security of dams, energy infrastructures, chemical facilities, buildings, and communities has been enhanced by the application of the process.

1.8 REFERENCES

1. Biringer, Betty, *Risk Assessment Method for Electric Power Transmission,* presented at Carnahan Conference on Security Technology, sponsored by IEEE, Albuquerque, NM, October 2004.

2. MIL-STD-882D, *Department of Defense Standard Practice for System Safety*, February 10, 2000.
3. *North American Electric Reliability Council, Urgent Action Cyber Security Standard,* Standard CIP-002-1, Draft, May 9, 2005, http://www.nerc.com/~filez/standards/Cyber-Security-Permanent.html.
4. *Sandia National Laboratories Security Risk Assessment Methodologies*, http://www.sandia.gov/ram.
5. Wyss, Gregory, D., "Risk Assessment and Risk Management for Energy Applications," in *Energy 2000: State of the Art*, ed. Peter Catania, Balaban Publishers, L'Aguila, Italy, pp. 163–184, 2000.

1.9 EXERCISES

1. Of what value is a security risk assessment to security risk managers? Justify your answer.
2. List and describe the parameters used to estimate security risk.
   a. Are these parameters mathematically independent? Why or why not?
   b. Can these parameters be quantified? Why or why not?
   c. Must these parameters be estimated in any given order? Why or why not?
3. Discuss estimating the threat potential for attack:
   a. What are the limitations, if any?
   b. What are important considerations?
4. Discuss estimating security system effectiveness.
   a. Why is it important to consider both physical protection system effectiveness and cyber-protection system effectiveness?
   b. Discuss the relationship between security system effectiveness and adversary success.
5. Discuss estimating the consequences of adversary attack.
   a. What are some possible parameters to define or describe consequence?
   b. What are consequence mitigation features? Define and provide examples.
6. What choices do managers have if security risk level is deemed to be too *High*? Describe ways to reduce security risk.

7. Why is it important to consider all impacts when considering security system upgrades?
8. How are safety and security risk assessments alike? How are they different?
9. How might the results of a security risk assessment be used for security contingency planning? Security contingency planning describes procedures or features that are implemented during elevated threat conditions for events that are otherwise very *Low* likelihood but *High* consequence.
10. How might potential adversaries use either input information or results of the security risk assessment for a given site?