Lesson Proper for Week 15

Understanding the Security Policy Life Cycle

The development of a security policy follows a life cycle similar to that of software development and many other important long-term projects. A parallel example is a country's foreign policy. A nation's government might have a thorough approach for dealing with political, social, and economic situations in foreign countries, but any number of sudden changes can challenge that approach very quickly. The election of a new prime minister, the passage of a new law, a labor strike, the looming outbreak of hostilities, or the capture of a spy can trigger the need for an immediate change in foreign policy. Similarly, some software products seem to be in a state of constant flux. Updates, patches, service packs, and new versions are released on a regular basis.

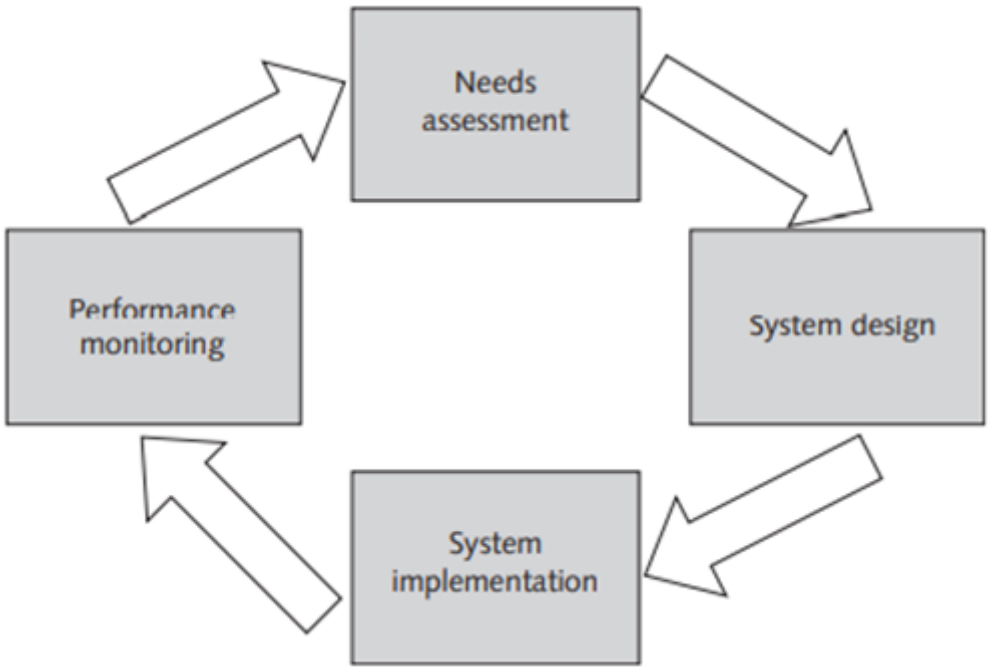

Figure 13-1 The system development life cycle

Needs Assessment

When developing a system or beginning a project, the first important question for an organization is to determine what it needs. The purpose of the system or project must be made clear. Inherent in this question is the issue of how to measure the project's success. Not all system development projects lend themselves to objective assessments, but some standards for success must be established.

System Design

Once the goal is clear, an organization can begin to create a system that addresses its needs. This phase includes planning. It is critically important to incorporate essential system elements at the beginning of a project rather than having to add them later. For example, it is very difficult to add security components to software after the code has been written; it is much easier to incorporate security as the code is written. Similarly, it is much easier to build legal and regulatory standards compliance into security policies than to rework the policies afterward. Thus, all stakeholders in a project should have input during the planning stage.

Once planning is complete, construction can begin. Whether the project requires writing code or creating security policies, a system of checks and balances should be put into place. For example, team members who are not directly involved in certain portions of a project should check the work of their colleagues in those areas.

System Implementation

Before a system is implemented, user training is often required. Training can be done in stages and using different processes. For example, training for top-level executives might be conducted earlier than training for front-line employees. Similarly, the depth and type of training needed may depend on job function. Typically, the time spent in training and the depth of that training is inversely proportional to an employee's position in the organization. Top-level managers receive less training than mid-level managers; department-level supervisors receive more training than mid-level managers but less than front-line workers. Depending on the project, a system might be implemented in a pilot phase and activated only with a limited scope, or a system might be rolled out completely and at once. New systems, including security policies, are often rolled out in stages, one department at a time, so that monitoring and needs assessment can proceed without affecting the entire organization. Department by department, the system is implemented.

Performance Monitoring

The monitoring phase can get lost in the press of other duties. Once a system is in place, it is easy to forget about it and move on to the next challenge if the system is not causing any obvious problems. In the case of security policies, this approach can be very dangerous. You may have created a policy for data backups that works well, but if you are not aware that software patches on the company systems have caused conflicts with the automatic backup software, you may be disappointed when you try to restore an important file that has been corrupted. If you are unaware of a change in a regulatory requirement or you missed the news that the accounting department modified a business process and thus subverted a security control inadvertently, your next external audit might be a shocking experience.

It is extremely important to the success of a project to monitor system performance continually. In the case of a security policy, you need to ask several questions: Are any of the assumptions made while developing the policy no longer true? Have new developments required modifications to the policy? Are employees compliant with the policy? Are managers enforcing compliance?

After answering the preceding questions and others, you may find that new needs must be addressed in the policy. Thus, you return to the needs assessment phase and the cycle begins again. Systems development, including security policy development, is an iterative and continual process: It cycles through needs assessment, system design, system implementation, and performance monitoring.

Examining the Concepts of Risk Analysis

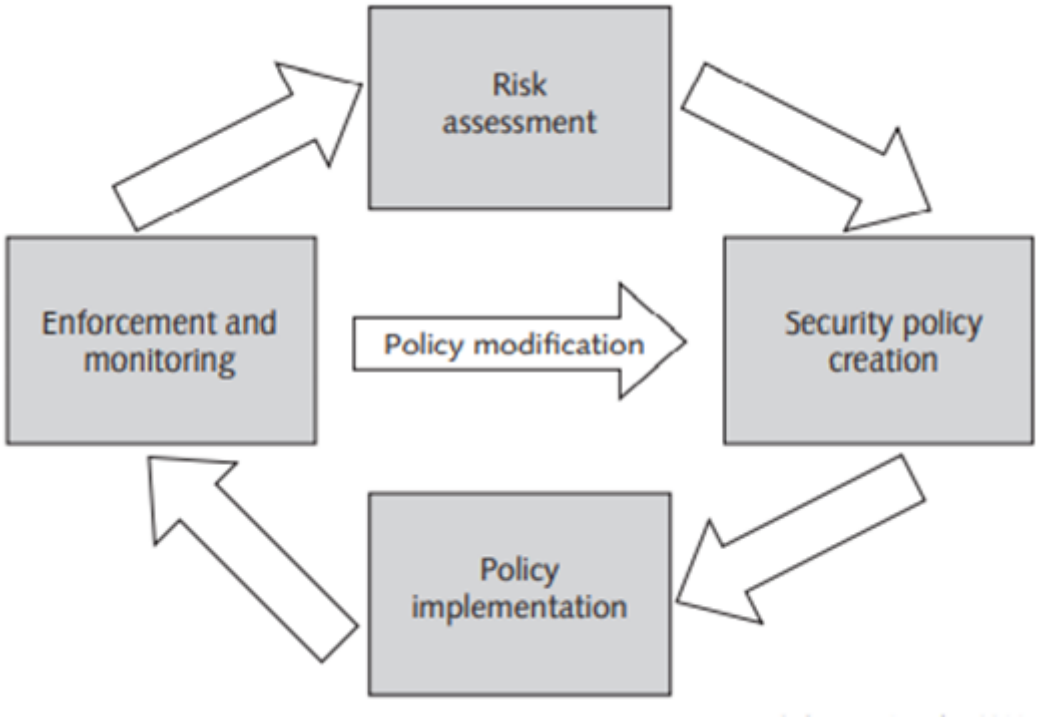

Figure 13-2 The risk analysis life cycle

Risk Analysis Factors

In terms of a network connected to the Internet, risk analysis should encompass computer hardware, software, and data warehouses—storehouses of valuable customer, job, and personnel information that a company needs to safeguard.

The following sections describe the six factors needed to create a risk analysis:

- Assets
- Threats
- Probabilities
- Vulnerabilities
- Consequences

- Security controls

Assets

Assets in an organization play a central role in risk analysis—after all, they are the hardware, software, and informational resources you need to protect by developing and implementing a comprehensive security policy. You are likely to encounter four types of assets:

- Physical assets—Equipment and buildings in the organization
- Data assets—Databases, personnel records, customer or client information, and other data the organization stores and transmits electronically
- Software assets—Server programs, security programs, and other applications used to communicate and carry out the organization's typical activities
- Personnel assets—People who work in the organization as well as customers, business partners, contractors, and freelance employees

Threats

Threats are events and conditions that could potentially occur, and their presence increases risk. Some dangers are universal, such as weather-related disasters. Others are more specific to your system, such as a server storing a customer database; an attacker could exploit the server to gain access to the system. Other examples of threats include the following:

- Power supply—The power supply in your area might be unreliable, making your company subject to brownouts, blackouts, and sudden surges called voltage spikes.
- Crime rate—If you work in a high-crime area or other offices in your area have been burglarized, your risk increases.
- Facility—If your building has old wiring that is prone to fluctuations or has insufficient fire suppression, the risk of fire damage increases.
- Industry—If your organization operates in a highly competitive industry or one that requires high security, a security breach could result in litigation or major loss of revenue or even force the business to close.

Probabilities

Geographic or physical location, habitual factors, and other factors affect the probability that a threat will occur. A geographic factor might include earthquakes, which are common threats in some regions. Physical location might also influence threat probability; an example would be an electrical problem in the building that houses your systems. Habitual factors could be poor security practices, such as employees keeping written passwords exposed near their computers that increase the probability of a security breach. These factors are a large part of what risk assessment seeks to uncover. Risk analysis evaluates each factor and rates its potential impact or exposure.

Threat	Probability
Earthquake	Medium
Fire	Low
Flood	High
Attack from the Internet	Very high
Virus infection	Very high
Employees giving out information	Low

Table 13-1 Sample threat probabilities

Vulnerabilities

Vulnerabilities are situations or conditions that increase the probability of a threat, which in turn increases risk. Examples include connecting computers to the Internet, keeping computers in open areas where anyone can use them, and installing Web servers outside the corporate network in the vulnerable demilitarized zone (DMZ).

Consequences

Substantial adverse consequences can result from a virus that forces you to take the corporate Web site offline for a week or a fire that destroys computer equipment. You can extend the earlier identification of threats to include ratings that evaluate consequences of those threats, as shown in Table 13-2.

Threat	Probability	Consequences
Earthquake	Medium	Significant
Fire	Low	Significant
Flood	High	Minor
Attack from the Internet	Very high	Serious
Virus infection	Very high	Serious
Employees giving out information	Low	Significant

Table 13-2 Probabilities and consequences of threats

Security Controls

Security controls are countermeasures you can take to reduce threats, such as installing firewalls and IDPSs, locking doors, and using passwords and encryption. These measures interact with each other to help manage risk. When deciding how to man- age risk, you must first identify and classify the risks. Next, you determine priorities of threatened assets, and then you determine whether to accept, transfer, or mitigate the risk.

An asset has an associated amount of risk. Threats and vulnerabilities increase the risk; countermeasures work to reduce risk. Residual risk is the amount left over after counter- measures are implemented; a risk never actually equals zero. Figure 13-3 illustrates this process.

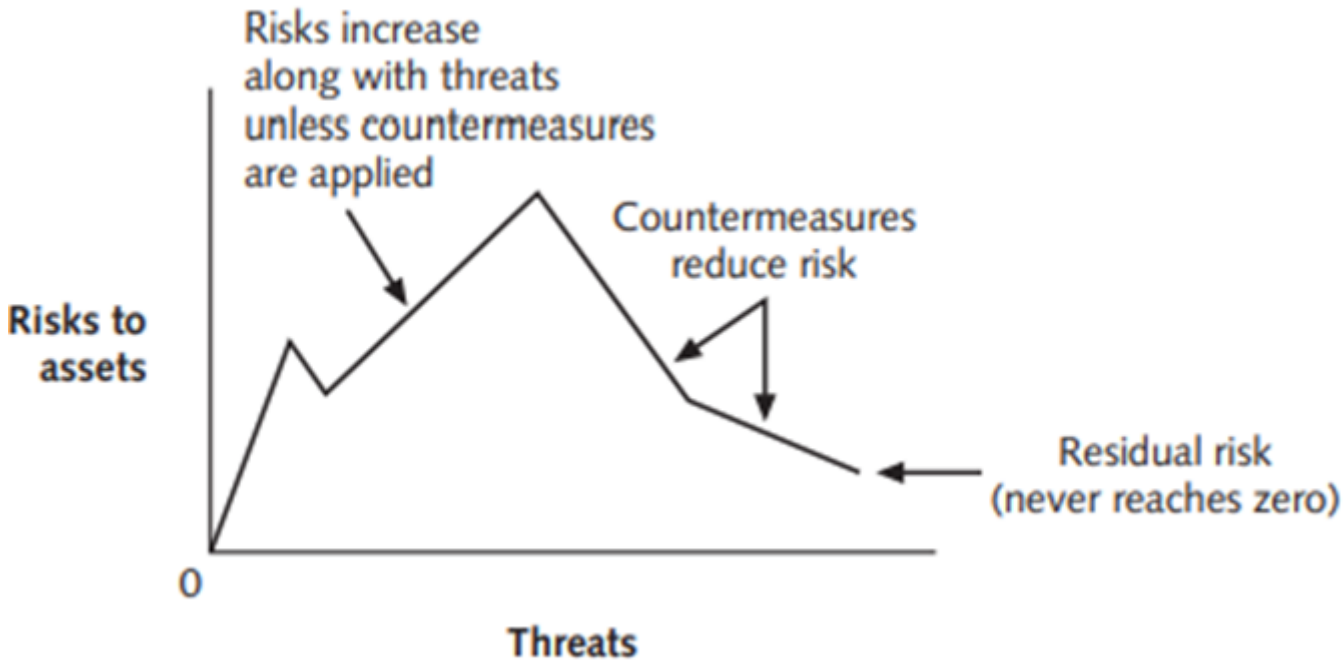

Figure 13-3 Countermeasures reduce but never eliminate risk

Survivable Network Analysis

Survivable Network Analysis (SNA) is a security process developed by the CERT Coordination Center. SNA starts with the assumption that a computer system or network will be attacked. It leads you through a four-step process designed to ensure the survivability of a network if an attack occurs. Survivability is the ability to continue functioning during attacks, system faults, accidents, or disasters.

Survivability focuses on a network's essential services, assets, and critical capabilities and depends on four key properties of a network:

- Resistance—The capability of a system to repel attacks
- Recognition—The capability to detect attacks when they occur and to evaluate the extent of damage and compromise
- Recovery—The capability to maintain essential services during an attack and restore all services afterward
- Adaptation and evolution—The capability to improve system survivability based on knowledge gained from attacks

Threat and Risk Assessment

Threat and Risk Assessment (TRA) approaches risk analysis from the standpoint of threats and risks to an organization's assets and the consequences if those threats and risks occur. Like SNA, TRA has four steps:

- Asset definition—You identify the software, hardware, and information you need to defend.
- Threat assessment—You identify the kinds of threats that place the asset at risk, including vandalism, fire, natural disasters, and attacks from the Internet. Threat assessment also includes an evaluation of the probability and consequences of each threat.
- Risk assessment—You evaluate each asset for any existing safeguards, the severity of threats and risks to each asset, and the consequences of the threat or risk taking place. The combination of these factors creates an assessment of the actual risk to each asset.
- Recommendations—Based on the risks and current safeguards, you make recommendations to reduce the risks. These recommendations should then become part of a security policy.
- Table 13-3 lists ratings you can assign to describe the probability of threats occurring.

Rating	What it means
Negligible	Unlikely to occur
Very Low	Likely to occur only two or three times every five years
Low	Likely to occur within a year or less
Medium	Likely to occur every six months or less
High	Likely to occur after a month or less
Very High	Likely to occur multiple times per month or less
Extreme	Likely to occur multiple times each day

Table 13-3 Describing the probability of threats

After rating the severity of a threat or risk, you evaluate the consequences if it actually occurs. Table 13-4 shows one method of describing consequences.

After evaluating the level of threats to assets and describing the consequences of the threats occurring, you can combine these two ratings to develop a risk analysis of each asset, as described in the following section.

Description	Consequences
Catastrophic	Threatens the continuation of the program and causes major problems for customers
Major	Threatens the continuation of basic program functions and requires intervention by senior-level management
Moderate	Does not threaten the program; however, the program could be subject to major review and modification of operating procedures
Minor	Could threaten the program's efficiency or effectiveness but can be handled internally
Insignificant	Can be handled by normal operations

Table 13-4 Describing consequences

The Risk Analysis Process

Risk analysis is not a one-time activity used to create a security policy. Rather, risk analysis evolves to account for an organization's changing size and activities, the progression to larger and more complex computer systems, and new threats from inside and outside the corporate network.

The initial risk analysis is used to formulate a security policy; the policy is then enforced and security is monitored. New threats and intrusion attempts create the need to reassess the risk an organization faces.

General Activities to Follow Risk analysis is a group of related activities that typically follow this sequence:

- Holding initial team sessions—First, hold meetings to get groups of workers together in one place. Conduct interviews or hand out questionnaires to collect pertinent information. It is especially important to talk to all managers to set the objectives and scope for the risk analysis, schedule how long the project should take, and identify the important people you need to interview.

- Conducting asset valuation—After you determine the scope of the risk analysis, you need to identify assets to protect and determine their value. This activity can be classified as subjective or speculative. If the activity is subjective, you are assessing the impact of losing assets that might not be tangible, and you should use your best judgment or solicit opinions from other qualified employees. If the activity is speculative, you are trying to determine whether information might fall into the hands of unauthorized people and estimating the cost of recovering the information. Personal interviews with managers can help you determine a realistic assessment.

- Evaluating vulnerability—You investigate the levels of threat and vulnerability in relation to the value of the organization's assets. Ask IT staff to evaluate the threat of virus attacks or other intrusions on a scale of one to five, for instance.

- Calculating risk—After you have determined asset values and the vulnerabilities that threaten those assets, you can calculate risk. Usually, a numeric value is assigned. For instance, 1 might represent a low-level baseline security need and 7 might represent a high-security priority.

Navigation

Home
Dashboard
Site pages
My courses
Capstone Project 2
Network Defense and Remote Access Configuration
Participants
General
15 [Enter Module Title Here]
Preliminary Activity for Week 15
Lesson Proper for Week 15
Analysis, Application, and Exploration for Week 15
Generalization for Week 15
Evaluation for Week 15
Assignment for Week 15
OJT/Practicum 2
Seminars and Tours
Courses

Fair Warning

Activities

- Assignments
- Forums
- Quizzes
- Resources