3 Security Methodology: Linking People, Processes, and Technologies

3.1 INTRODUCTION 3-1
3.2 PUTTING THE PIECES TOGETHER – A METHODOLOGY 3-2
3.2.1 Overview 3-2
3.2.2 Description of the Methodology 3-3
3.2.3 Step 1: Develop Model of a System 3-5
3.2.4 Step 2: Establish a Management Approach 3-6
3.2.5 Step 3: Local Risk Analysis 3-6
3.2.6 Step 4: Global Risk Analysis Through Attack Trees 3-7
3.2.7 Step 5: Development of Countermeasures and Risk Mitigation 3-10
3.2.8 Step 6: Updating System Designs 3-11
3.2.9 Conclusions 3-11
3.3 CONTINUING CASE STUDY: SECURITY FOR NRW (NERVOUS WRECK, INC.) 3-11
3.3.1 Overview 3-11
3.3.2 Step 1: System Conceptual Model 3-12
3.3.3 Step 2: Establish a Management Approach 3-12
3.3.4 Step 3: Detailed Local Risk Analysis 3-14
3.3.5 Step 4: Global Risk Analysis through Attack Trees 3-16
3.3.6 Step 5: Choosing Enabling Security Technologies as Countermeasures 3-18
3.4 CHAPTER SUMMARY 3-19
3.5 REVIEW QUESTIONS AND EXERCISES 3-19

3.1 Introduction

This chapter discusses a methodology that combines management approaches, security requirements, risk analysis, and circumventions into a systematic procedure. The procedure is explained through a detailed example that is expanded in later chapters.

Chapter Highlights

- Many approaches developed for information security
- Most have the following steps:
  - Develop and deploy an overall security management approach with policies, procedures, roles and responsibilities.
  - Establish security detailed requirements that include internal as well as external

factors. These requirements drive the security initiatives.
  - Conduct risk and threat analysis to understand the vulnerabilities. A variety of techniques are used in this step. Attack trees are one of the common techniques.
  - Develop circumventions and policies to mitigate risks. The emphasis on policies versus technologies may vary depending on the type of threat, but both are needed.
- Numerous variations and customizations of the aforementioned steps exist. SAM (system assurance Methodology) is one of them.

3.2 Putting The Pieces Together – A Methodology

3.2.1 Overview

Several methodologies, formal as well as informal, have been reported in the literature for security and information assurance. An example is the Red Team methodology used in several defense-oriented projects. This methodology shows how a Red Team, a team of trained security professionals, can audit the security of a system. It also provides a useful and broad characterization of possible attack types. Another example is the work of Volkmar Lotz, "Threat Scenarios as a Means to Formally Develop Secure Systems" (LICS 1146, 1996; also a Munich Ph.D. thesis). However, Lotz's method is a formal method that is based on streams of messages communicating over channels. Threat scenarios are given abstract characterizations as streams, and they interact with streams abstractly representing system behavior. The following discussion is an extension of the System Assurance Methodology (SAM). The objectives of SAM are :

- Identify typical significant threats and, in a systematic way, characterize likely attacks to IA systems relative to their missions and designs.
- Characterize adversaries by their motivation, objectives, resources, tolerance for risk, and required access to targeted systems; i.e., develop a theory of adversarial behavior in terms of the attacks they are likely to mount.
- Characterize countermeasures systematically by the burdens they place on systems in development and in operation, and by the effects they have on attack characteristics and the resources required by adversaries to exploit vulnerabilities and execute attacks.
- Characterize systematically threats, likely attacks, and countermeasures over time during the evolution of IA systems.
- Characterize gaps and needed remedies in the IA Program as the result of finding specific threats, likely attacks, and countermeasures.
- Determine measurable positive changes in IA systems as they evolve.
- Assist in the strengthening of systems through design changes to counter given threats and likely attacks.
- Provide help in determining the direction and progress of the IA program.
- Provide a means for strategic planning for IA systems.

3.2.2 Description of the Methodology

figure 3-1 shows a simplified view of a security methodology based on SAM. The methodology starts with a clearly stated mission statement and a system design (or architecture) for the system under consideration. The main steps of the methodology are:

1) Build a model of the system that includes design/architecture of the system under consideration. See section 3.2.3.

2) Develop a management approach that starts with identifying the most valuable assets and establishing requirements to protect them. Based on this, policies, controls, and other organizational procedures are developed. See section 3.2.4.

3) Do "local" risk analysis that analyzes vulnerabilities of *individual* valuable assets. These vulnerabilities can be described in terms of PIA4 or in terms of the Orange Book levels of trust (see the sidebar, "Orange Book Security Levels"). See section 3.2.5.

4) Do a detailed analysis of global risks by analyzing possible attacks that may involve multiple resources and steps. This also includes a model of attacker behavior with some idea of adversary objectives, and of the likelihood of the adversary having requisite capabilities, system access, and tolerance of the risk of detection. This step is important because it considers stealthy attacks in which the attacker takes advantage of relative weaknesses of multiple systems to reach his/her goals. Attack trees, described in section 3.2.7, can be the foundation of global risk assessment.

5) Develop countermeasures (risk mitigation approaches) to survive the attacks. The effectiveness of countermeasures is gauged according to cost, performance, functionality, and ease of use. The countermeasures, discussed in section 3.2.7, use the policies and security technologies we have reviewed in previous sections.

6) Update the system on the basis of the likely attacks and countermeasures. The desired result of the system update is a stronger system together with some assurance evidence. This sounds obvious, but in some cases, the updated system is weaker because the updates are too complicated and leave several security holes. See section 3.2.8.

7) Go back and reiterate the steps to modify the model to reflect the changes; re-visit the management approach; and conduct more in-depth analysis with new attackers, different systems, different attack trees, etc.

This generic iterative process can become more formal as it proceeds. In the initial iterations, the process can begin with informal brainstorming sessions for systematically validating a security design for a system with respect to an adversary and likely vulnerabilities. In the later iterations, the process can become a security testbed with automated aids.

The main idea is to build survivable systems that can tolerate attacks by working through various attack trees systematically (Schneier 1999). Success of this process is measurable by the overall advance of the system and its resistance to, or ability to deal with, further attacks that might not have been considered explicitly. In other words, after a few iterations, the system should have been updated to the point where it can tolerate and survive almost anything (famous last words!).

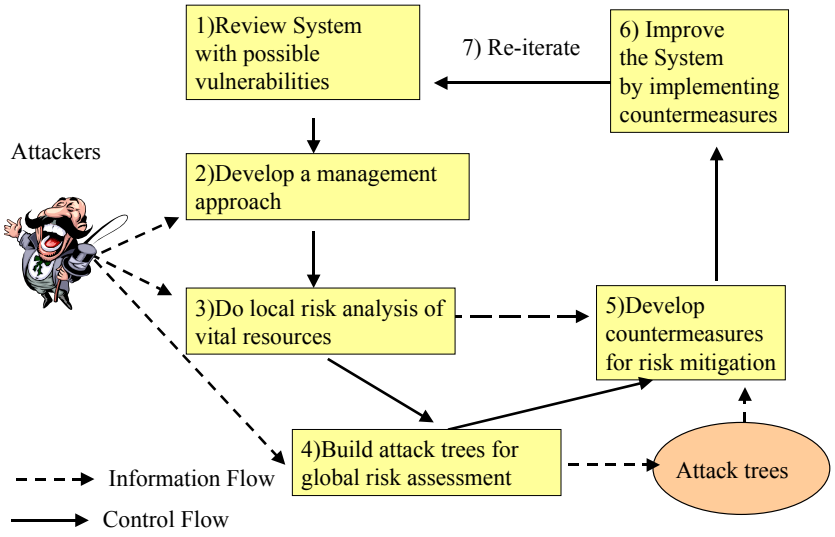

figure 3-1: A Simple Methodology

Orange Book Security Levels

The DOD (Department of Defense) has defined seven levels of Trusted Computer System Evaluation Criteria, otherwise known as the Orange Book. Although originally written for military systems, the security classifications are broadly used in the computer industry.

The DoD security categories range from D (Minimal Protection) to A (Verified Protection). The levels are used to evaluate protection for computing hardware, software, and stored information. The security levels are additive—higher ratings include the functionality of the levels below. The definitions are built around access control, authentication, auditing, and levels of trust. Here is a summary:

D: Minimal Protection. This indicates that the system is insecure. D-level certification is very rare because this is essentially no security at all.

C: Discretionary Protection. This applies to systems with optional object (i.e., file, directory, devices, etc.) protection. C1 and C2 are subcategories of C. C1 is the lowest level of security and indicates that the system has file and directory read and write controls and authentication through user login. However, auditing (system logging) is not available. C2 provides an auditing function to record all security-related events and provides better protection on key system files, such as the password file. C2 is one of the most common certifications. Examples of operating systems are: VMS, IBM OS/400, Windows NT, Oracle 7, and others.

B: Mandatory Protection. This level supports multilevel security. B1 provides secret, top secret, and mandatory access control, which states that a user cannot change permissions on files or directories. B2 states that every object and file be labeled according to its security level and that these labels change dynamically depending on

what is being used. B3 extends security levels to the system hardware. For example, terminals can only connect through trusted cable paths and specialized system hardware to ensure that there is no unauthorized access.

A: Verified Protection. This is the highest security division. A1 is the highest level of security validated through the Orange Book. The design must be mathematically verified; all hardware and software must have been protected during shipment to prevent tampering. This level of protection requires significant central processing unit (CPU) processing power and disk space. Enabling these security features may seriously affect the performance of low-end computers and devices.

Sources for Additional Information:

http://www.dynamoo.com/orange/summary.htm

http://www.iec.org/online/tutorials/int_sec/topic01.html

3.2.3 Step 1: Develop Model of a System

The model of the system must show the important components and their interrelationships. The view should show the overall architecture of the system under consideration. The description of the system may be formal or informal. The level of details may depend on the type of analysis. For example, figure 3-2 shows a conceptual model of an online purchasing system that can be used for high-level analysis. figure 3-3 shows a physical model of the same online purchasing system with a multi-tiered architecture in which the back-end systems reside on a mainframe system, and the catalog is on a Solaris machine, but the Web server itself runs on a Windows NT server. Numerous middleware and network components are also shown because these are all possible attack points for an attacker. For detailed security analysis, detailed models of this nature are typically needed. We will develop, analyze, and explain detailed technical models in Part III and Part IV of this book (if you do not understand it right now, relax!).

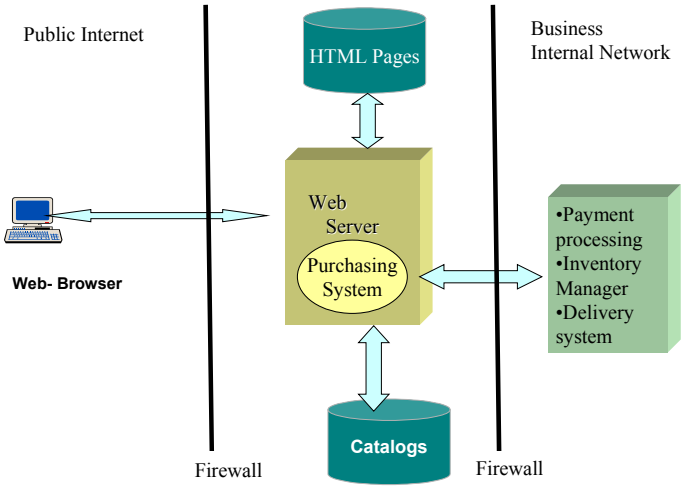

figure 3-2: Conceptual Model of an Online Purchasing System

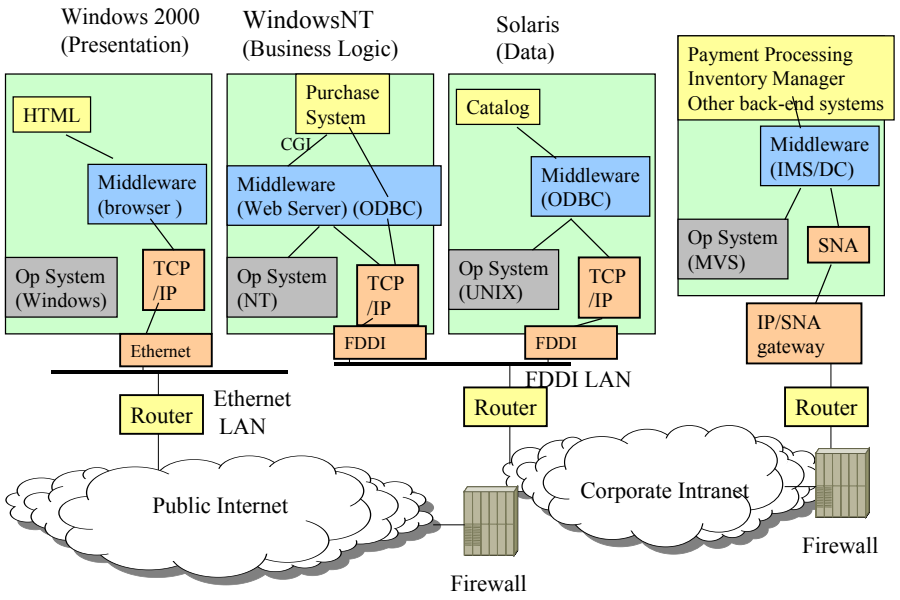

figure 3-3: Physical Model of an Online Purchasing System

3.2.4 Step 2: Establish a Management Approach

It is important to develop organizational policies, roles, and training programs before choosing the security technologies. For a comprehensive security solution, enterprises need to develop security management approaches that:

- Establish general security policies and enforce them through controls and audits
- Develop organizational roles and responsibilities
- Institute security awareness and training programs
- Establish security requirements based on external (e.g., regulations) and internal considerations
- Conduct risk analysis to understand the vulnerabilities
- Develop circumventions and policies to mitigate risks

We discussed the management approach and these activities in the previous chapter. The main responsibility of managers is to develop an approach that secures the enterprise assets by developing and enforcing proper policies, controls, and audits that are essential without creating unnecessary bureaucracies.

3.2.5 Step 3: Local Risk Analysis

Risks associated with each valuable resource needs to be evaluated. Basically, local risk analysis involves a study of vulnerabilities of individual system components, and identification of threats that could exploit the vulnerabilities. Vulnerabilities and threats can be discussed in terms of privacy, integrity, authentication, authorization, accountability, and availability ***(abbreviated PIA4).*** PIA4 can be applied to any

component (database, access point, application server, network segment, etc). For example, in case of a completely wireless and mobile environment, we could describe these vulnerabilities in terms of the following system components:

- Wireless networks (e.g., wireless LANs, cellular and satellite networks)
- Wireless middleware and mobile application servers such as WAP and Sun J2ME
- Applications and data that are accessible from wireless communications

These system components need to be protected against the following type of attacks, expressed in terms of PIA4:

- Privacy attacks – unauthorized reading of information while it is in a system or in transit.
- Integrity attacks – unauthorized modification of information while it is in a system or in transit.
- Authentication attacks – forging user IDs or PWs
- Authorization attacks – unauthorized access to a component
- Accountability attacks – not leaving any trace of who has done what
- Availability attacks – jamming/flooding/crashing the components to cause availability issues

We discussed risk analysis in the previous chapter. The results of the risk analysis can be represented in terms of the following risk matrix:

R(i,j) where:
i = component id (may be an application, a database, an access point, a WAP gateway, a router, or a backbone network segment)
j = security id such as privacy (j=1), integrity (j=2), authentication (j-3), etc.

R (i,j) reflects the business risk associated with particular resources (components) for different types of attacks and could drive the protection needed. For example, a financial database may need higher risk because of its content, a network segment may be at higher risk because of its use, etc. The entries of R may be L, M, H, or numeric values. For instance, R (2,1) = H indicates that a component 2 is at high risk against privacy (j = 1) type attacks. See the NRW case study later in this chapter, and local risk analysis in section 3.3.4, for an example of R.

It is important to note that local risk analysis should include non-IT along with IT components. In particular, it is essential to conduct risk analysis of components such as power supplies and physical room locations. It should also be emphasized that a good local risk analysis can make the task of global risk analysis much easier. In particular, many possible branches of attack trees, discussed next, can be quickly pruned as a result of thorough local analysis. For example, if a database has been secured in local risk analysis, then we can bypass the branches of attack trees that lead to this database, thus reducing the size of the attack trees.

3.2.6 Step 4: Global Risk Analysis Through Attack Trees

Most security attacks are stealthy and not directly detectable. In fact, sophisticated attackers could launch a series of atomic attacks which may themselves not seem to cause any harm but could gradually force the system to reach an unsafe position. In such cases, the attacks can be represented as state transitions. Attack tress, also known as attack graphs, represent such transitions.

An attack tree, introduced in the previous chapter, is a convenient way to explore potential attacks and thoroughly examine the "attack space." An attack tree is simply a tree that is similar to a logical decision tree used to perform a systematic analysis of the attack space. The attack tree may be represented through a graph or some other means such as the extended outline mode of Microsoft Word. Attack trees are built by considering the "what," "where," "when," and "how" of attacking the system. For "what," an attacker can try to compromise system and data integrity, data confidentiality, or system availability. For "where," an attacker could attempt to do this inside a firewall (an internal attacker), at the firewall that separates the internal system from the public Internet, or on the public Internet. For "when," an attacker could mount the attack at any point in the lifecycle of the system, during system design and development, during system operation, or after the system has exceeded its useful life and is being discarded. The "how" of an attack deals with the mechanism used to execute the attack, such as eavesdropping.

Let us consider the online purchasing system shown in figure 3-4. Attack trees can be built for each security concern: privacy, integrity, and availability. The following is a simple attack tree or piece of an attack tree for an online purchasing system:

C What: Confidentiality of data in the Purchasing System

C1 Where: Inside the Purchasing firewall (the when and how for later analysis)

C2 Where: Between Purchasing System and the Internet

C2.1 When: During system development

C2.1.1 How: Inadvertent human attack

C2.1.1.1 How: Coding error in purchasing access software

C2.1.2 How: Deliberate human attack

C2.1.2.1 How: Malicious code inserted in purchasing software

C2.2 When: During system operation

C2.2.1 How: Inadvertent human attack

C2.2.1.1 How: Sensitive information included in query[1]

C2.2.2 How: Deliberate human attack

C2.2.2.1 How: Sensitive information included in query

C2.2.3 How: Deliberate software attack

C2.2.3.1 How: Sensitive information included in query

C2.2.3.2 How: Malicious software returned to purchasing with query results

C3 Where: On the Internet

[1] The DARPA Information Assurance program is specifically focussed on deliberate attacks. However, an IA analyst may need to consider inadvertent "attacks," such as operator error, when designing a system.

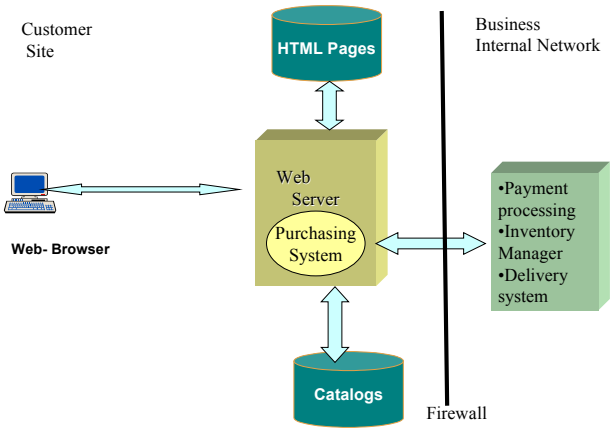

figure 3-4: Online Purchasing System

In building attack trees, an analyst uses knowledge of the mission and knowledge of threats to determine which branches of a tree to explore in depth, and which branches not to pursue or to prune early in the analysis. Naturally, judgment and knowledge are critical to the overall assurance of the system. Pruning a tree branch early can result in missing a critically important attack that develops deep in the tree. However, because attack trees would be extremely large for most systems, it is imperative that the trees be pruned as early as possible to keep the analysis manageable. The leaves of attack trees are indicators of attacks. Each attack characterizes the risk and should help in determining countermeasures. The table below lists all the attacks from the tree above.

Table 3-1: Confidentiality Attack Tree

Attack	Description
C2.1.1.1	Sensitive information is inadvertently released from Web server to the Internet due to a software coding error by a person during development of the purchasing system
C2.1.2.1	Sensitive information is released from purchasing to the Internet via malicious software inserted in the purchasing system by a person during system development
C2.2.1.1	Purchasing system administrator inadvertently includes sensitive information in a query sent to the Internet
C2.2.2.1	Purchasing system administrator deliberately includes sensitive information in a query sent to the Internet
C2.2.3.1	Malicious software in the Business Internal Network includes sensitive information in software-generated queries sent to the Internet
C2.2.3.2	A response to a purchasing query returns malicious software in addition to the requested data. The malicious software installs itself in the Business Internal Network and leaks sensitive information to the Internet

In addition to confidentiality, there may be concerns about other security properties. Similar trees can be built for availability and integrity.

The attack tree shown above has been heavily pruned during construction. Prudence is needed before pruning because once pruned, the pruned attacks are excluded from future analysis. An important objective of the tree is to provide a heuristic for systematically considering attacks. A fully developed tree should have a complete listing of attacks but

may be too big. Partial construction or pruning should be done carefully because the determination of which branches not to follow is based on a conjecture of adversary behavior. It is quite difficult to guess adversary behavior – they may act "rationally" according to commonly accepted "rational standards" or may act rashly or "out of character" in various cases or extreme conditions. It is quite possible adversaries may do the unexpected when it leads to the desired objective. It is best to be as comprehensive as possible in building an attack tree and prune those leaves that have the least likelihood and/or impact.

A natural question is: can the attack trees be generated automatically? An interesting approach to automating this process has been reported by a group at Carnegie Mellon (Sheyner 2001).[2] A simplified version of this automated procedure is:

- Start with an initial state S0.
- Identify the set of atomic attacks and number them (0-5, let us say). Each attack has a set of preconditions.
- From the initial state S0, launch attacks that meet the precondition and result into next state S1.
- From S1, launch next attacks that meet the precondition, etc.
- Keep repeating until you reach an unsafe condition.
- All unsafe conditions are reached this way and the paths to these unsafe conditions comprise the attack trees.

3.2.7 Step 5: Development of Countermeasures and Risk Mitigation

The security designers develop countermeasures from their knowledge of the possible attacks and of the security technologies and approaches that can help an enterprise survive the attacks. There can be many countermeasures for a given attack. As stated previously, countermeasures may include:

- Policies that mitigate risks by stipulating consequences and transferring risks through insurance.
- Technologies that protect the assets through encryption, password protections, audit trails, etc. These technologies protect the important resources by strengthening the privacy, integrity, and other PIA4 aspects. We will discuss these technologies in part II of this book.
- Use of other instruments such as intrusion detection systems (IDSs) and honeypots. IDSs are designed for continuous monitoring and detection of intruders (see chapter 5 for details). Honeypots are built especially to attract the intruders and keep them busy or frustrate them with nuisances (see chapter 14 for details).

From these possible countermeasures, a suitable one is chosen based on cost, functionality, performance measures, ease of use, and effectiveness in dealing with the corresponding attack. For comparisons among countermeasures, it is desirable to choose the countermeasures that increase the costs and capabilities needed by the adversary and also increase the risk of detection. The comparative analysis should lead to the most appropriate countermeasures being implemented for risk mitigation. A major concern is

[2] Sheyner, O., et al, "Automatic Generation and Analysis of Attack Trees," http://www.cs.wisc.edu/~jha/jha-papers/security/oakland_2001.pdf

to cohesively design the great many countermeasures that could cover the many likely attacks. The main challenge is: how will the countermeasures fit with each other and also with other functions of the system, while maintaining the mission of the system and keeping within reasonable developmental and operational costs? For a unified design approach, there will be a considerable number of value judgments about the countermeasures and how they fit into the overall system. For example, different cryptographic techniques can be used as countermeasures but need to be evaluated against cost and performance issues (e.g., symmetric versus asymmetric, key length impact, etc.).

3.2.8 Step 6: Updating System Designs

The chosen countermeasures, when added to the current system design, lead to an updated system design. This is also a creative rather than an algorithmic process. Retaining the mission and the main functions of the system should be key factors in updating the system design. There may be compromises so that some degradation of some functions of the upgraded system is acceptable. For example, strong encryption can degrade the performance of a system.

The updated system will need to be assessed to determine whether it is acceptable or not. The assessment will include several factors, such as preservation of the primary mission and confinement of implementation and operational costs of the redesigned system. If the updated system is not acceptable, then the information assurance process should be re-applied. Being unacceptable means that the system does not satisfy the functional, performance and security requirements. Even when the updated system is acceptable, it is extremely unlikely that it will be a perfect system that is completely impervious to all attacks.

3.2.9 Conclusions

Methodologies such as the one discussed above are guided steps that the user can follow systematically. The main advantage of this methodology is that it combines a management approach with technical solutions. It is also risk-driven and the use of attack trees keeps us close to the central problems of securing systems against the attacks of malicious adversaries. The methodology is also iterative. It would be a good idea to automate some parts of the process. For example, the attack trees can be built from a system diagram. However, it is not clear how to automate the process of constructing countermeasures and picking the right ones that lead to a highly survivable system.

3.3 Continuing Case Study: Security for NRW (Nervous Wreck, Inc.)

3.3.1 Overview

NRW is an investment firm that has been bought by XYZCorp. With partners in the US and Europe, NRW wants its customers to access and update their account information and use some of the firm's financial analysis tools via the Internet. The goal of the

company security system is to reduce the cost of customer service while ensuring customer and company data are secure *and* recoverable. While there are many design areas at play in this company, the focus here is on security. In particular, the objective is to develop a management approach by using the methodology described in the previous section. The approach should include:

- Security requirements
- Security risks
- Organizational structure, awareness policies, roles and responsibilities
- Risk analysis and key security technologies as countermeasures

3.3.2 Step 1: System Conceptual Model

Let us start with a conceptual model of NRW shown in figure 3-5. The NRW corporate web site consists of a user interface that connects to an Accounts Balance Program (ABP) that allows customers to view, update, and modify account information; a customer database that contains information about customers; an investment database that contains investment data; and other typical corporate applications and databases for payroll, accounts payable/receivable, etc. A corporate network will operate in the building, connected to the public Internet. A firewall protects the internal corporate resources. This simple model will be sufficient to get us started.

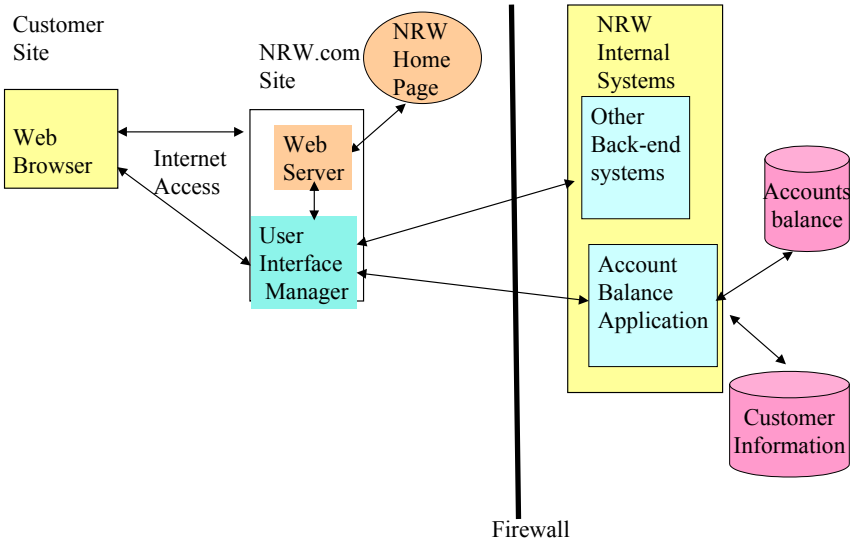

figure 3-5: NRW System Conceptual View

3.3.3 Step 2: Establish a Management Approach

3.3.3.1 High-Level Risks and Requirements

With the implementation of a web portal for account management, NRW will be potentially exposing itself to several security risks. Moving the customers away from telephone support and to the Internet has obvious benefits (24x7 service, more support

with fewer staff); however, it introduces several risks at a high level, such as the following:

- Denial of service can happen due to any number of reasons. For example, network outages and network flooding, viruses, hackers and physical equipment problems could all deny users the ability to conduct business with NRW.
- A web interface will open the company up to assaults from outside parties looking to disrupt NRW's business.
- Access to individual accounts will increase the risk of manipulation of account data by customers.
- Unauthorized users may access information on customers, accounts and research.
- Hackers can attack using falsified authentication.

Should any of these events occur, NRW will risk damage to its internal systems and also to its reputation, resulting in significant loss of business.

A sound management approach is needed by the organization to address these and other risks. Integral parts of the management approach are the organizational structure of the security team, the awareness policies distributed to the employees, and the different roles and responsibilities of each team member.

3.3.3.2 Organizational Structure

One of the key elements of the successful implementation of the security program is to define the organizational structure. The organizational structure will ensure the effectiveness of NRW security. The NRW system administrator is responsible for creating and maintaining the security model. Different organizational units within the NRW corporation will support the Account Balance Program (ABP) shown in figure 3-5. A corporate Chief Security Officer (CSO) is responsible for the security and the integrity of all NRW systems. It is the CSO's job to watch out for the Account Balance Program. The CIO will be more hands-off and will work with the CSO and other managers who manage NRW resources such as the network, databases, and applications.

As the organization grows, an information security coordinator in every business unit within NRW may be very effective (initially security coordination may be just a function assigned to an area manager). While the CSO would be responsible for the overall implementation and running of the security program, the information security coordinators provide the day-to-day decisions within each business unit, and then report to the CSO. Also, the supporting level personnel would bear responsibility for implementing the overall security awareness program.

3.3.3.3 Security Awareness Approach

NRW's CSO will have to raise company awareness of the security, especially of the ABP. This may be done through required courses or internal marketing within the firm via emails and written memos. The firm should clearly inform the employees, through the training, about what they may access and the penalty for any security breach. The training, procedures and guidelines will help NRW to be able to maintain the desired level of security. Specifically, the following approach is suggested before the implementation of security measures and technologies:

- The security plan should be presented to all existing NRW employees, as well as to the newcomers, on a regular basis.

- All current training needs of NRW employees should be identified, and presented to the CIO by the CSO. If possible, every business unit security coordinator should contribute to this report.
- The security plan should be presented, after approval, on a regular basis such as twice a year, to ensure that all newcomers as well as existing employees are aware of the plan.

Several companies can provide security training. Examples are the Computer Security Institute and Learning Tree, Inc.

Special control measures will be needed to keep the information security awareness plan alive and effective. These could include unexpected "security audits" of security procedures; after-hours visits to IT department employee offices to check if the required security procedures are being performed; and regular (twice a year) organization of "Security Alert Days" with different security issues (e.g., viruses) on the agenda.

3.3.3.4 Roles and Responsibilities

The roles and responsibilities of the different team members need to be established. Of course, the CSO is responsible for maintaining the overall coordination of NRW's security. It is expected that the CSO will disperse the responsibilities among various employees. This is to ensure that no single person has too much control over the system. This benefits the firm in that it better maintains security, and allows for protection from vulnerability if that person were to leave the job. The best way for NRW to establish this is to rotate the responsibilities among the different team members.

The level of security in every business unit will be implemented according to the roles and responsibilities of user segmentation. The factors to be included are: level of awareness needed versus level achieved; job category and specific job function; familiarity with systems; and areas of expertise.

3.3.4 Step 3: Detailed Local Risk Analysis

The NRW Web customer interface will result in an unlimited number of potential interactions from an unlimited number of potential sources. The security requirements must not simply protect information from getting into the wrong hands. They must also assure that the system survives successful attacks and keeps providing services. This security plan increases the scope of protection to include a course of action in the event of a breach of security or failure of a certain level of service. Thus Information Assurance will be employed in order to accomplish both objectives. Specific security measures to be implemented must provide the following:

- Authentication and validation of internal and external users; e.g., unauthorized access to NRW's corporate information systems should be prohibited.
- A simplified user interface for authentication, to maintain high user satisfaction.
- Rigorous access control so that only authorized users can access and modify account information.
- Quick detection and denial of service to unverified users.
- Ensure that users are provided with 24x7 access.
- The system must be recoverable quickly; i.e., backup and recovery procedures must be in place.

- High availability of systems should be guaranteed through use of techniques such as Fragmentation, Redundancy, and Scattering (FRS).

By providing users with high availability, the need for large customer service resources will be reduced, lowering costs and achieving one of the major goals of the initiative.

Let us specify detailed risks for the key components by developing the risk matrix R(i,j) for components i (business service, host, router, physical connection) and vulnerabilities j (privacy, integrity, and the rest of PIA4). Before developing R, let us just realize that the NRW system components need to be protected against the following type of attacks:

Privacy attacks – unauthorized reading of information while it is in a system or in transit

- Access to individual accounts will increase the risk of manipulation of account data by customers.

Integrity attacks – unauthorized modification of information while it is in a system or in transit

- Attacks using falsified authentication by hackers

Authentication attacks – forging user IDs or PWs

- Access to individual accounts will increase the risk of manipulation of account data by customers.
- Unauthorized users may access information on customers, accounts and research information.
- Attacks using falsified authentication by hackers

Authorization attacks – unauthorized access to a component

- Authentication and validation of internal and external users; e.g., unauthorized access to NRW's corporate information systems should be prohibited.
- A simplified user interface for authentication, to maintain high user satisfaction.
- Rigorous access control so that only authorized users can access and modify account information.
- Quick detection and denial of service to unverified users.

Accountability attacks – not leaving any trace of who has done what

Availability attacks – jamming/flooding/crashing the components to cause availability issues

- Denial of service can happen due to any number of reasons. For example, network outages and network flooding, viruses, hackers and physical equipment problems could all deny users the ability to conduct business with NRW.
- A web interface will open the company up to assaults from outside parties looking to disrupt NRW's business.
- Ensure that users are provided with 24x7 access.
- The system must be recoverable quickly; i.e., backup and recovery procedures must be in place.
- High availability of systems should be guaranteed through the use of techniques such as Fragmentation, Redundancy, and Scattering (FRS).
- By providing users with high availability, the need for large customer service resources will be reduced, lowering costs and achieving one of the major goals of the initiative.

The risks associated with these attacks can be represented in terms of the risks matrix R(i,j). For the NRW example, we can develop Table 2 to reflect the security riskss R for a few major components – the rows – that are important for us: the account balance program, and the database. For these components, the risks are specified in terms of PIA4 – the columns. Risks for additional components, and sub-components, can be similarly specified. In addition, it is possible that R(i,j) may be an overkill and could be aggregated by a vector R(i) that captures the overall security risk of component i. Notice that the Account Balance Program (ABP) is at higher risk because it is accessed from external users. However, the Account Balance Database has lower risk because it is only accessed from an internal "trusted" program (ABP) and is not directly accessible from an external user.

Table 2: Example of a Security Risks Matrix R

	Privacy Risks	Integrity Risks	Authentication Risks	Authorizatio n Risk	Accountabilit y (NR) Risks	Availability Risks
Account Balance Application	M	H	H	H	M	H
Account Balance Database	H	H	M	M	M	M

3.3.5 Step 4: Global Risk Analysis through Attack Trees

The main idea of detailed risk analysis is not only to identify the threats but also to develop countermeasures to combat them. The main objectives of this analysis are:

- To identify potential threats and describe them as real possible attacks on different NRW systems in different business units.
- To describe the possible behavior of the systems under attack, in order to identify the gaps in defense and to develop the defense strategy.
- To determine the time lapse between the attack and recovery, frequency of the attacks, possible places of the attacks, etc.
- To evaluate the effectiveness of the defense measures and to assist in the strengthening of the systems.
- To connect the management approach to an implementation.

To determine the possible attacks on the system, we first review the NRW system design and then develop "attack trees" that are built by considering "what," "where," "when," and "how" of attacking the system. For purpose of illustration, we will use the conceptual view presented in figure 3-5. Before developing an attack tree, let us look at the what, where, when, and how at a high level.

What: What parts of the architecture could be at risk for security breaches?

- Web Server and network. Denial of service, hacked entry with intent to do harm or gain information
- Institutional Databases: This includes all user personal and financial information as well as corporate information and directory database.
- Routers and gateways: could be passageways into the extranet and Intranet

Where: Where will these breaches or attempts take place?

- Hackers may pinpoint individual systems or components
- Localized to the web servers or network routers or gateways
- Internal espionage and eavesdropping

When: When would a possible attack take place, and with what frequency?

- During normal operations
- After hours; batching or back-up
- While in development, rollout or switch over

How: How will these risks be assessed and mitigated?

- Assessed by a total loss basis
- Multiple redundancies will help secure system

Attack trees can be built for each security concern: privacy, integrity, and availability. An example of building the privacy attack tree for NRW confidentiality of data is presented below (note that this is very similar to the attack tree developed for an online purchasing system in section 3.2.6):

```
C What: Confidentiality of data in the NRW System

      C1 Where: Inside the NRW firewall

      C2 Where: Between NRW Web Server and the Internet

        C2.1 When: During system development

                C2.1.1 How: Inadvertent human attack

        C2.2 When: During system operation

                C2.2.1 How: Inadvertent human attack

                        C2.2.1.1 How: Sensitive information included in query

                C2.2.2 How: Deliberate human attack

                        C2.2.2.1 How: Sensitive information included in query

                C2.2.3 How: Deliberate software attack

                        C2.2.3.1 How: Tapping the line, especially in case of a

                        wireless network

      C3 Where: On the Internet
```

This tree focuses on confidentiality attacks against the interface between NRW server and the Internet. The attacks are the last leaves of the tree (C2.1.1, C2.2.1.1, C2.2.2.1, C2.2.3.1).

In addition to confidentiality, there may be concerns about other security properties. The tree below explores some aspects of service assurance due to denial of service on the NRW system:

```
S1.     What. Service Assurance of System Threatened – Denial-of-Service
Attack on System
S1.1.   Where. Individual Component or Subsystem
S1.1.1.Where. End system
        S1.1.1.1. When. During network operation
```

```
                    S1.1.1.1.1.     How. Passive attack
                    S1.1.1.1.1.1.   How. Eavesdropping
                    S1.1.1.1.2.     How. Active attack
                    S1.1.1.1.2.1.   How. Illegal logon or system entry as user
                    or root to cause denial of service
                    S1.1.1.1.2.2.   How. Dial-port flooding
                    S1.1.1.1.2.3.   How. Shutdown
            S1.1.1.2. When.         During development …
        S1.1.2.         Where. Router
        S1.1.2.1.       When. During network operation
        S1.1.2.1.1.     How. Passive attack
        S1.1.2.1.1.1.   How. Eavesdropping (preparing for DoS attacks)
        S1.1.2.1.2.     How, Active attack
        S1.1.2.1.2.1.   How. Attacks on routing protocols
        S1.1.2.2.       When. During development …
```

The attack tree below shows some aspects of availability:

```
A What: Availability of NRW System access to the Internet

      A1 Where: Inside the NRW firewall

      A2 Where: Between NRW Server and the Internet

        A2.1 When: During system development

A2.1.1 How: Insert time-bombs in NRW network or flood the network

        A2.2 When: During system operation

                A2.2.1 How: Disrupt critical network services such as DNS

A2.2.2 How: Flood Web access ports

                A2.2.3 How: Introduce malicious code into NRW

A3 Where: On the Internet
```

Both the confidentiality tree and the availability tree shown above have been heavily pruned during construction. For example, the "where" branch of the availability tree that examines attacks occurring inside the NRW firewall is ignored. This may or may not be a prudent decision. By pruning this branch early in the analysis and excluding any such attacks, the remainder of the analysis will not consider this option, and countermeasures will not be chosen against this type of attack.

3.3.6 Step 5: Choosing Enabling Security Technologies as Countermeasures

NRW will establish some key attributes of the security architecture for the Accounts Balance Program (ABP) to address the risks identified above (high-level as well as low-level) through attack trees. We will discuss these topics after we have reviewed the security technologies in the next part of the book. See the continuation of NRW Case Study at the end of Chapter 6.

3.4 Chapter Summary

Security management is an important part of enterprise security. It is needed to protect the corporate IT and physical assets by using policies and employing the latest security technologies to respond to external factors and organizational requirements. This chapter has given a short overview of management issues with a discussion of policies, requirements, and risk assessment. A methodology that puts these issues into a systematic procedure concludes this chapter.

3.5 Review Questions and Exercises

1) How would you customize and upgrade this methodology to handle extreme security situations, such as FBI information systems, and very light security needed for situations such as chat groups?

2) Take another example and work through the steps of the methodology.

3) How can attack trees be used to identify risks, analyze them, and then mitigate them? Give an example.

4) Compare and contrast the Orange Book Security Levels with PIA4. Is there any relationship?