Chapter 10

General IT Security Plan

Solutions in this chapter:

- IT Security Assessment and Audit
- Authentication
- Access Control
- Auditing
- Attacks
- Assessment and Audit Report
- General IT Security Project Parameters
- General IT Security Project Plan

☑ Summary

☑ Solutions Fast Track

Introduction

In this chapter, we provide the framework for creating a general Information Technology (IT) security project as part of your overall corporate IT security project plan strategy. As with all of the individual security area projects (ISAPs) discussed in this book, this is intended to be a template to use as a starting point. You might be wondering what a "general" IT security project plan consists of. In this chapter, we'll discuss the security assessment and auditing function in great detail. Most corporate IT security plans start with a thorough assessment so that the problem statement can be developed. As discussed in Chapter 9, you might perform your assessment as one of the major objectives of your corporate project, or you might implement the assessment as a separate project whose results feed into your corporate IT security project plan. Either way, your planning begins with an assessment, which is covered in detail here. We also look at access control, authentication, and attacks, and how to build a project plan that addresses these core areas.

IT Security Assessment and Auditing

For the purposes of this chapter, let's define assessment as the act of testing network security to determine the strength of current security measures. Furthermore, let's define auditing as the act of examining, recording, and evaluating security configurations. Clearly these two activities should work in tandem. If all you do is run some tests against your network, you've performed an assessment that might yield important information. However, if your test misses some critical area, you're still vulnerable. If you perform an audit, you might see that your server configuration is air-tight. Again, you might miss a vulnerability caused by the interaction of security in one network system (e.g., servers) and another network system (e.g., firewalls or routers). These two activities are, in a sense, two sides of the same coin and together they provide as complete a picture of your network security as possible. Let's begin by talking about assessments.

People are always the weakest link in security. Take the recent cases of hackers getting into corporate credit card databases. In many of these recent stories, someone on the inside of the organization made a poor decision (whether malicious or not) about how to handle the data, resulting in a vulnerability that was exploited by an outsider. Social engineering, lack of awareness of security best practices, and malicious intent are ranked very high on the list of vulnerabilities from the people perspective. Assessing your vulnerabilities from a people perspective should include these methods.

Processes are the security processes maintained by the company from top to bottom. Vulnerabilities occur because IT security processes, such as analyzing key network traffic, are poorly defined or poorly executed. Corporate policies with regard to security processes often fall behind known threats and fail to address new threats. A good example is having a policy about reporting new or unexpected equipment found on or near one's desk. Since rogue wireless networks are easy to install, if employees are not vigilant about investigating new or unusual equipment (they often assume someone from IT put it there), there is a risk. In addition, if IT policy doesn't specifically define a procedure for installing new equipment, you are losing an opportunity to maintain security. It's a two-sided process. IT should define clear procedures for how things will work, so that users can be educated as to standard operating procedures. Both groups can therefore keep an eye out for rogue or unusual activity that falls outside standard policies and procedures. In addition, processes such as how employees are removed from access control lists when they leave the organization, should be part of the assessment to ensure standard procedures maintain strong security.

Technology vulnerabilities are the most tangible of the three vulnerabilities and are the ones that most people in IT start out looking for. While these are found in abundance in technical trade magazines and Web sites, don't make the mistake of thinking that the most important vulnerabilities are those with the actual technology. While important, they are part of this triad of people, process and technology that, when addressed holistically, gives your network the highest possible security. In many ways, assessments, access control, authentication, and auditing address all three aspects of security. There are technology assessments and risk assessments, both of which are discussed in this section.

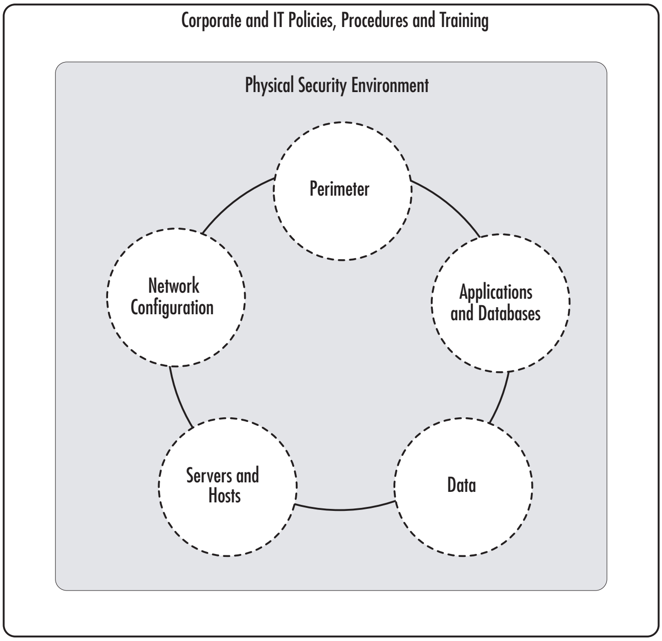
Business Intelligence…

Lingo

For what it's worth, the National Security Agency (NSA) and the National Institute of Standards and Technology (NIST) use slightly different lingo. They use management (people), operations (process), and technology. In *How to Cheat at IT Project Management* and throughout this companion book, we use the terms people, process, and technology, which are slightly different but the intent is the same.

We can also look at security through a layered approach. In fact, the more ways you parse out your environment, the more likely you are to find vulnerabilities. In Figure 10.1, you can see that your first line of defense consists of your policies, procedures, and user awareness. These form the foundation of all network security, because people and process are two of the three major components of security. The physical environment includes physical access to equipment and the general security of the facility. If a hacker gains legitimate (though unauthorized) access to someone's desk and is able to root around amongst all the sticky notes to find a username and password, you essentially have wasted all those thousands (or millions) of dollars on protecting the network from outside attack. Finally, there are both physical and virtual security elements related to the perimeter, the internal network, servers and hosts, applications and databases, and the data itself. The virtual elements include all the ways someone could access this information from outside the organization, while the physical elements include the ways someone could physically access these components.

Figure 10.1 Layered Approach to Network Security


Corporate and IT Policies, Procedures and Training
Physical Security Environment
Perimeter
Applications and Databases
Data
Servers and Hosts
Network Configuration

Perimeter or Boundaries

First, you should define your perimeter and determine where your border areas are. (Some people use the term "perimeter," and others prefer the term "boundaries.") Be clear that the perimeters or boundaries are either physical or logical. The port of a router is a physical boundary. A network segment is a physical boundary. The Internet Protocol (IP) subnet is a logical boundary. The responsibility for securing data from Point A to Point B is a logical boundary. Next, you should define the components that protect your perimeter, which typically include firewalls, routers, proxy servers, and Demilitarized Zones (DMZ's), to mention a few. After user awareness and adherence to policies and procedures, your perimeter defense is often your first line of defense against external attacks. Remember, many attacks or security breaches are internal, so an obsessive fixation with just the perimeter is not going to keep your network safe.

Internal Network

How your network is configured and segmented is of great interest to hackers, because once they learn this, they can navigate easily through your entire internal network. Information regarding the segmentation and addressing of network segments as well as the presence and configuration of any network intrusion detection systems (IDS), would also be a real bonus for a hacker, and would provide a great jump start to many types of intrusive attacks.

Servers and Hosts

Information about the types, locations, and numbers of servers and hosts (for our purposes, any non-server network device with an IP address,) is great information for a hacker. This is an area where a fair amount of effort is expended to harden the devices against attack. System hardening includes tasks such as disabling unused protocols and ports, removing unused applications, implementing access control and authentication requirements, maintaining up-to-date anti-virus, anti-spyware applications, maintaining up-to-date operating systems and applications, and performing ongoing and meaningful intrusion detection and auditing functions.

Applications and Databases

Applications and databases are also common targets for attackers. If a hacker can gain access to an application, he or she might be able to modify data, insert data, or steal data. The same holds true for a database application except that with databases, there is often a wealth of information a hacker would really like to get their hands on. In addition, sometimes the objective is to simply corrupt the database to cause financial or political problems for the company. Think of a database used for an online application in which a hacker changes the product pricing or inserts bad language into the product description. Think of a database that becomes corrupted, and mailings regarding the results of Human Immunodeficiency Virus (HIV) testing are mailed to people's work addresses instead of home addresses. The list of possibilities is endless, and part of your assessment should be how the data could be corrupted and what the potential implications of such a result would be.

Data

Ultimately, hackers want data of all kinds. Sometimes the hacker doesn't know exactly what data he or she wants, but they'll take whatever they can get their hands on. Sometimes there's a ripple effect to data acquisition. A hacker might start with just the name of a technical contact listed in the WHOIS database for a Uniform Resource Locator (URL). He then uses that information to call the company and, through social engineering, convince the technical contact to give him the username and password for the account on the hosting company's Web site. He or she then logs on and installs some tracking software. Now, every time a customer logs into his or her account on your Web site, the bad guy gets instant access. Clearly, this is just one type of data a hacker can use, but you can see how it can ripple down into your organization.

Unfortunately, there is a lot of public information out there on both publicly and privately owned companies. There is no way to avoid that. However, a good rule of thumb is to only disclose required information, and to verify the entity you are disclosing the information to. Let's look at some of the kinds of data a hacker might put to use.

Contact Information

As mentioned, various kinds of contact information can be extremely useful to attackers. They can use it to represent themselves as an employee or agent of the company, or they can use it to talk to the internal contact directly, pretending to be a legitimate external representative of a service provider. Employee names, mailing addresses, e-mail addresses, and phone numbers are excellent resources for social engineering.

Business Information

Who are your company's business partners? Who are your vendors, suppliers, and contractors? This information is also extremely helpful for an attacker, because it can be used to impersonate people with legitimate ties to your company. In addition, if your company is acquiring or divesting another company or division, it creates security holes that can be exploited by an attacker who is aware of this activity.

Extranet and Remote Access

While extranets and remote access channels are great tools for employees and vendors for a variety of purposes, unfortunately they are also magnets for hackers. Especially vulnerable are accounts used by external business partners, which typically use weak or default passwords. Unused or forgotten modems are another great source of unauthorized remote access.

Valid User Accounts

To a hacker, valid user accounts with passwords are the mother lode, but even just a valid user account is a great starting point. It provides the attacker with information about the format of your user accounts and allows them to quickly figure out other valid user names based on the contact information provided. Some companies use a different username format than their e-mail addresses to protect the user login format information (e.g., your e-mail address format might be *first initial_lastname@yourcompany.com* whereas your user login information might be *first name_middle initial_first four letters of your last name*. While it's a bit more difficult for users to remember, they'll quickly get the hang of it. It won't necessarily prevent a hacker from figuring out your username format, but it might slow them down a bit. It might also help you to see any attempts at brute-force attacks, if they follow the format for your e-mail addresses and not your standard username format.

If an attacker has a valid user account and can figure out the format, he or she can then start a brute-force attack to crack the password. Thus, protecting user account formats is one half of the equation; the other half is requiring strong passwords.

System Configuration

System configuration information is also extremely valuable to an attacker, because he or she can determine what types of attacks to launch. If someone knows you're running Microsoft Windows Server 2003, he or she can specifically attack vulnerabilities of those systems, including exploiting systems that have not been kept up-to-date with critical security patches. An example of this can be found at www.netcraft.com.

Business Intelligence…

Deterrence Tactics

An alarm on your car doesn't prevent it from being stolen, it simply deters the would-be thief. They have to think twice about whether or not they can boost your car before someone pays attention to the alarm. Similarly, protecting your corporate data from attacker reconnaissance missions is not going to increase your security, it will simply help deter would-be hackers. Putting up barriers wherever you can without impeding your own business processes (or without unduly impeding users) reduces the chances that an attacker will select your network as a target. In the end, your layered security systems are what will protect you, but why not make it as difficult as possible for a would-be attacker to get any helpful information?

Types of Security Assessments

There are various types of assessments you can perform on your overall network security. We're not going to go into complete detail here, because these topics are large and ever-changing. However, there are two major categories worth addressing: vulnerability scanning and pen testing.

Vulnerability Scanning

Vulnerability scanning slices both ways. You're doing it to keep the bad guys out and the bad guys are doing it to find a way in. From the IT administrator's perspective, the goal of vulnerability scanning is to identify devices on the network that are open to known vulnerabilities. Despite your best efforts, there will always be new vulnerabilities discovered, and your activities in this area will likely be almost non-stop. However, you have to begin from a known starting point, and performing vulnerability scanning begins with addressing the obvious first. Also, keep in mind that vulnerabilities encompass people, processes, and technology, so be sure to look at all three areas when addressing vulnerabilities. It doesn't matter how locked down your systems are if you have a power user lose a laptop or hand out a password to someone posing as an IT staffer. Also, keep in mind that penetration (pen) testing is not useful for scanning for vulnerabilities if the system hasn't been secured. Other methods are more productive on the front end; pen testing can be more helpful on the back end after security measures have been implemented.

Enumeration

The most common type of vulnerability scanning is done using software tools that attempt to enumerate, or list, all of the network components. Enumeration includes scanning to identify network segments, IP ranges, IP addresses, network configuration, names, addresses, and version numbers for network devices, protocols, ports, versions, users, groups, directories, patches, updates and any other information about the network. Enumeration is possible because system vulnerabilities lead to unauthorized exposure of important system information and because system capabilities are actually designed to help administrators manage networked systems, which also helps attackers. When vulnerabilities exist, they allow for exposure of information that can be exploited by an attacker.

Security Mistakes

Most organizations have a lot of data stored in various locations, directories, and servers across the enterprise. Are you absolutely sure each of those areas is properly secured? Systems are often configured to replicate settings from the top of the hierarchy down through the lower layers of the directory or file hierarchy. Did those settings replicate properly? Were the original settings correct, or were mistakes replicated throughout the organization as well? These kinds of security mistakes can create huge security holes; therefore, vulnerability scanning should look for weak passwords, incorrect user, file, or folder permissions, default configurations, and unused features that should be disabled. In addition to errors, you also need to ascertain whether any settings have been altered or modified by a user within your organization. If a user's permissions were accidentally misconfigured, he or she may have had the ability (even if for a short time) to increase their permission levels or even create a new user account for themselves.

Known Vulnerabilities

Known vulnerabilities are the first things exploited by attackers, but they're also addressed by software makers through patches and updates. While a vulnerability might become known before a patch is available, often the patch is available before the attacker finds your network and your vulnerability. Such was the case in 2003, when the Blaster virus hit many corporate networks. The patch had been available for about three weeks before the attack occurred, but many organizations' computers were not patched; best estimates place the infection rate at about 500,000 computers. Patching and updating are important in addressing known vulnerabilities, and since 2003, most organizations have developed better systems for patch and update management. Microsoft has new tools available, including the automatic update feature on desktop systems and the Microsoft Security Baseline Analyzer tool that allows you to scan for known vulnerabilities from a Microsoft systems perspective. Some scanning tools look for registry settings to determine whether or not the system is up-to-date, and more extensive programs attack the system via the known vulnerabilities to see how it responds. A wide variety of tools are readily available and are usually a good investment for companies of all sizes. However, remember, these tools are also available to the bad guys.

Common Attacks

Vulnerability scanning has to look at both sides of the equation. Are known vulnerabilities addressed? Are known attacks addressed? There are many known attacks and attack methods that should be addressed in your security assessment. It's not enough to cover known vulnerabilities; it's possible that if you simulate attacks on your network you may uncover previously unknown vulnerabilities. Not all vulnerabilities can be patched or updated. Some vulnerabilities are the result of the interaction of two or more network components or systems. Therefore, it's important that you include common attack scenario testing in your security assessment.

Pen Testing

Pen testing by itself proves nothing. So what if you can penetrate an insecure network? It's akin to walking in the open front door of a house; it doesn't tell you if the locks work. Second, pen testing is by no means comprehensive. In fact, it is like a laser; it goes directly at a particular target in a very focused manner. It will give you a result based on a specific circumstance, but it won't give you a broad overview of your network security. If you're going to use pen testing as a tool, start with the "low hanging fruit"; in other words, make sure the front door is locked, and then work your way up from there. Performing pen testing after a security project is far more useful than doing it beforehand, so be sure you understand when and why you'd use pen testing in IT security projects. Be clear about what the results of a pen test will tell you, not what you assume they'll tell you. As an assessment tool, pen testing should be limited in scope (e.g., if you believe some specific part of your network is locked down you might perform a pen test on that area to verify your assumption).

Pen testing can be a tricky area, because you essentially have to hack your own network. So, before you head off to do a pen test, make sure you have the appropriate sign-off from corporate executives. The last thing you need is for you or one of your staff to be falsely accused of attacking the network when, in fact, you were legitimately testing the security of the network. Having a security testing plan in hand and getting sign off from your project sponsor is the best way to ensure there are no negative repercussions. Also keep in mind that an inexperienced pen tester could cause unintended problems ranging from minor to severe. Think carefully about how and when these tests should be carried out and by whom. If you retain an outside firm to perform this type of testing, be sure they come well-recommended and with the appropriate credentials and a spotless reputation. Also, make sure that they sign the appropriate paperwork to shield you and them from liability. Finally, keep in mind that many companies think that hiring an outside firm to "just do the pen testing" is sufficient. What they fail to realize is that performing pen testing absent other security planning and implementation activities, can actually lay the company wide open for legal liability. If you are aware of the problem but do not take "reasonable care" in addressing it, you could be worse off than not knowing about the vulnerability in the first place.

Keep in mind that the ultimate goal of pen testing is to obtain administrator-level privileges. Therefore, your testing should start from the same place as an outsider—without a username or password. Pen testing usually tries to exploit known vulnerabilities first, so this is a logical place to start. Not all vulnerabilities can be addressed, however. Remember, there is a limit to what you can protect and what you should protect. In keeping the balance between security and cost and security and reasonable business operations, you will probably find yourself making conscious trade-offs between security and other business objectives. Therefore, you may have to be creative and find alternate ways to address vulnerabilities besides simply closing and locking the door on them.

There are various methodologies you can use to perform a pen test. Here's one to get you started:

1. Think like the attacker. Determine how the attacker would most likely try to attack your network. This normally begins by locating all publicly available information on the target and using that information as a starting point.
2. Locate vulnerabilities and areas of weakness. Use the elements in Figure 10.1 to ensure you're looking across the entire enterprise.
3. Determine all the ways (currently known) a hacker could exploit the vulnerabilities and weaknesses found in Step 2.
4. Determine which assets might be attacked to access, alter, or destroy data based on the likely attack scenarios defined in Step 1 and the vulnerabilities identified in Step 2.
5. Determine whether an attack can be detected. If you are performing a pen test, determine if you were able to detect the attack, either in real-time or in retrospect.
6. Determine the attack footprint. The attack footprint is the size of the target. If you're shooting an arrow, it's harder to hit the stem of a plant than the side of a barn. The same holds true for your network. Determine how big a target you're providing.
7. Analyze results, formulate remediation strategy, and implement.

Risk Assessment

We know there is a trade-off between total security and total risk. There are financial and operational trade-offs that every organization must make. In the risk assessment phase of your audit, you need to look at your risks in four specific categories: *asset protection, threat prevention, legal liabilities*, and *costs*. This is a good time to sit down with key stakeholders, including your executive sponsor or team, your financial, legal, human resources, and operational experts to determine what your company's specific risks are. As mentioned in Chapter 5, your IT security project plan team membership will likely change as you move through the phases of your project. Risk assessment is a part of the initial definition stage, and should include all of the key stakeholders you can think of. At this point, it might be better to invite too many people to attend this meeting rather than too few. Anyone who finds their participation is not needed can opt-out, but you want to avoid forgetting a key player who can help you and your IT team perform a thorough risk assessment.

The risk assessment itself should be thorough; skimp here and you will likely end up with a less-than-optimal security solution. Even if your company can't afford to implement all the recommended security solutions, at least you'll have a thorough assessment of what's needed. This may be important later on, because if a security breach does occur, you can point to documentation showing that your assessment indicated the breached area was a risk (which might save your job down the line). However, rather than be right later on, use the results of the assessment to pro-actively push for a bigger budget and implement those changes now. If there's documentation showing that you were aware of the potential security risk and did not implement a solution, your firm might have a huge legal and financial liability on its hands. So, the thorough assessment cuts both ways. It gives you the data you need to make your case for appropriate funding, but it can also be used by attorneys to prove your company was aware of the risk and chose not to act.

Risk Assessment: Asset Protection

As we have continually stressed throughout this book, you have to find the right balance between protecting corporate assets and the cost of doing so. In any network assessment scenario, you should begin by understanding what you're trying to protect and why. You may have adequately addressed this issue during your overall IT corporate security planning process. If so, you should review the data, assumptions, and outcomes at this stage to ensure your conclusions are still relevant and correct. Things change so quickly in most corporate environments, that a quick review of previous assessment data is almost always a good use of your time. You should review what data is on your corporate network and what needs to be protected. This is also a good time to find out what is on your corporate network that perhaps should not be. If you recall the case studies from Chapter 1, it's not uncommon for corporate networks to store confidential data on the corporate network, such as credit card numbers or social security numbers.

In addition to discovering what is on your network (and what's there but shouldn't be), you also need to assess the relative value of that data. While it can be argued that all corporate data is valuable, some data is clearly more valuable than other types of data. Remember that you need to think like a hacker to make these assessments. A list of nuts, bolts, and cable lengths are not worth as much in value as personal data such as credit card numbers, social security numbers, and bank access codes. Correlate the data on your network with the perceived value of the data to an outsider, to understand the relative risk to your network. This will help you determine how much security is appropriate for your specific situation.

A good example of this is a home wireless network. Most people using home wireless networks for things such as logging onto their online brokerage account or doing some online shopping with a credit card, do not secure them. This data is transmitted in an unsecured manner from their laptop or wireless device to their wireless access point, and then to the router or cable modem and out to the Internet. How likely is it that a hacker is going to grab that data? If you live in a dense urban setting where a hacker can sit in a nearby coffee shop and peruse wireless data like yours, then the likelihood is high. If you live in a more suburban or rural setting where it would be difficult for someone to get close enough to receive your wireless signal, the risk drops significantly. If you're in an urban setting and you run an unsecured wireless network, your risk is probably four times higher than someone in a more rural setting. That said, your overall risk is still about 50 times lower than that of any corporate network, because a hacker would have to sift through a fair amount of mundane wireless traffic at someone's home before being able to grab usernames, passwords, and so forth; the upside potential for that hacker is minimal. Why go after a single person's data if you can access thousands or millions of people's data? Looking at the risk/reward proposition from a hacker's perspective will help you assess the relative value of your assets and what level of protection is warranted. Keep in mind there is always the hacker of convenience, who hacks because he or she can, whether there is a big payoff or not.

Sensitive Data

Sensitive data is defined differently from one company to the next. What's sensitive at one company may not be sensitive at another. However, in most companies, there are clearly segments of data that are sensitive and, therefore, your security audit should identify those areas. As part of your corporate security project plan definition stage, you must clearly understand how sensitive your corporate data is. It goes beyond the legal implications and into the business aspects. Lists of customers, vendors, suppliers, or employees can be sensitive, especially if you're in a medical setting. Trade secrets, formulas, and research and development (R&D) data can be extremely sensitive, especially in industries that work in leading edge or groundbreaking areas. This is a great place to get feedback and input from the various departments in your company. Ask them what data they work with that they would not wanted posted on a Web site or printed in a newspaper. That usually gets people's attention and helps them to begin looking at the data they work with on a daily basis from a slightly different perspective. Here's a quick list of data typically considered sensitive:

- Customer databases
- Employee lists
- Identity information (e.g., customer, employee, vendor)
- Credit card or other financial data
- Health information
- Intellectual property
- Trade secrets
- R&D

Remember, too, that there are two ways sensitive data is at risk. First, it can be stolen and used inappropriately by your competition, your employees, or by those who can gain financially from the data. Second, it can be compromised. Imagine the damage that could be done if a publicly held corporation's financial statements were changed without the company's knowledge, just before being released to the Securities and Exchange Commission (SEC) or just before a major announcement. Sensitive data must be protected from theft and from modification. Keep that in mind when you're looking at your corporate IT security auditing plans.

Network Services and Business Operations

Sometimes an attacker is less interested in stealing or compromising data than they are in disrupting business operations (e.g., shutting down a Web site through a Denial of Service (DOS) attack, or corrupting a customer database or modifying financial statements). Whether it's the external link (Web site) or the internal network, some hackers are simply looking to undermine the availability of the network. There are numerous areas to look for vulnerabilities in business and network operations. The following is a list to start with; your organization may have additional operations that need to be included on this list.

- Internet connectivity
- Web site connectivity
- Web-based applications
- Database services
- Directory services
- File services
- E-mail services
- Virus and intrusion prevention and detection services
- Custom application services
- Voice over IP (VoIP) services

Take an inventory of the various ways your company uses the network and electronic communications to understand the vulnerabilities that your corporate IT security project plan should address. More than likely, you'll want to create ISAPs to address the various categories, because smaller projects are more manageable.

Risk Assessment: Threat Prevention

Threat prevention starts with the IT security project problem statement. What problems are we trying to solve with this project? In other words, what threats do we perceive that we need to address? What is the company trying to protect through these security measures? What kinds of threats are likely or possible? Are you most concerned about an attack, a theft, or a breach and which is most likely to occur? Answering these questions will help you define your problem and your outcome statements, and will also help form a solid foundation for your corporate IT security project plan.

Because past security measures may be in place, there is not always a direct relationship between the importance of data and the threat to that data. If you process credit card transactions through a third-party company, you do not store the credit card data any longer than it takes to transmit it to that third-party company. Also, if all of your transactions are conducted using a secure Internet protocol (Hyper Text Transfer Protocol Secure sockets [HTTPS] and so forth), the risk of credit card data being stolen from your company is fairly low. When looking at your threats and vulnerabilities, you should rank both the importance (the relative financial value) of the data and the relative threat or risk to that data. You want to make sure your most important data is properly secured while also ensuring that your biggest vulnerabilities are addressed. By identifying vulnerabilities and their likelihood of occurrence, you can create a prioritized list that will help you make smart decisions should you be forced to choose to implement only a portion of your total corporate IT security strategy. If you need to stage your corporate IT security project implementation to meet the financial needs of the company (e.g., breaking it down into phases that can be funded each fiscal quarter), this prioritized list can also help you decide which projects should be addressed during each phase of funding.

Denial of Service

A DOS attack is usually launched at a company's Web site with the clear intention of making it unavailable to legitimate users. However, a DOS attack can also be launched in a variety of ways to deny service to Web sites, Internet access, network access, or wireless network access. When looking at your vulnerability to a DOS attack, don't just look at the risk to your Web site; look at the risk to any network component that provides vital business service that could be attacked.

Unauthorized Access

The threat of unauthorized access to network resources comes in various forms, all of which must be considered. It's important to assess any points of entry (e.g., the Web site, any dial-in communications that are still enabled (remember, you may not use dial-in access any more, but you may still have modems with live phone lines connected to your servers that have never been removed); network login and wireless access points are the most common. In addition, unauthorized access can be gained through various protocols being left open including Simple Network Management Protocol (SNMP), telnet, serial ports, and a variety of Transmission Control Protocol (TCP)/IP ports. Using default settings on routers and wireless access points also leaves you vulnerable to unauthorized access, as does providing more lenient access to users and user accounts than needed. Finally, there is the issue of social engineering that is often successfully used on sophisticated IT staff and unsuspecting users alike, in order to gain access to legitimate network credentials and to unauthorized.

Identity Theft

Identity theft is on the rise and while most people assume it happens as a result of online fraud, there are numerous ways identity theft can occur. However, we confine our discussion of identity theft to the kinds most likely to occur within the business environment. As we've repeatedly discussed, any company that collects, stores, or transfers credit card data can be a source of identity theft. In addition, companies that collect, store, or transfer other personal information including names with addresses, social security numbers, and various account numbers (mortgage, brokerage account, bank account, insurance, and so on) can also be a source for information used to steal someone's identity. It's also important to secure employee's personal data including the above-mentioned information, because even a company with 50 employees is a decent coup for someone attempting identity theft.

Individual consumers must take steps to secure and protect their personal information when interacting with businesses; however, even then there are limits to what a consumer can do. Take the well-publicized cases discussed in Chapter 1. Those are clear indicators that businesses are the more likely target for identity theft, since hackers would clearly like to get their hands on 100,000 names and not just one or two. It's critical that you take an inventory of the data your company collects, stores, and transfers, and identify any data that could be used to perpetrate identity theft on your consumers, your employees, or any other individuals your company deals with.

Personal Information Exposure

Personal information exposure can be the source of identity theft, but it's not exactly the same thing. Exposure of personal information could be private or personal data that would not necessarily facilitate identity theft but some other type of harm. For example, suppose a medical supply company's list of people and their associated medical problems was stolen and that the information was made public. That information couldn't be used to steal someone's identity, but it could reveal other personal information that customers don't want to share. If your company has any sort of sensitive information including age, marital status, vacation schedules, alarm codes, and so forth, your firm could be liable if that information is stolen and used in any malicious way. A recent episode of a new television program featured a group of robbers that broke into an architectural firm and stole blueprints to a bank. While such a robbery would be outside your control, if a hacker broke into your network and stole the electronic blueprints to someone's home, another company, or a financial institution, your company could be held liable for a related robbery.

At the risk of redundancy, review all of the data your company stores, even data that appears to be useless to outsiders, and think about how that data could be used if it fell into the wrong hands.

Credit Card Fraud

We've talked extensively about personal information and we've referred repeatedly to credit card information as some of the most sensitive information companies work with. For most hackers, the bigger the potential gain, the more desirable the target. Therefore, any company that runs an online store is clearly a more interesting target than a home computer. Online stores use secure Web protocols to ensure personal information, including credit card data, is secure when the user data is transmitted via the Internet to the company's Web site. Many smaller e-commerce sites use a third-party credit card processing company to handle the entire credit card transaction so that the data never sits on the company's server for more than the time it takes to authorize the transaction. Still, there is a vulnerability there. Hackers can compromise the Web site, redirect Web traffic, spoof the URL, send bogus e-mail that appears to be from your company and your Web site, redirect users to an alternate URL; the list goes on and on. Also, keep in mind that the threat is increased if you have an unsecured wireless network connected to your wired network. Any hacker than can gain access through the wireless network can work his or her way onto the wired network and into your credit card data.

Corporate Trade Secrets or Competitive Data

We can become so focused on personal user data such as social security numbers or credit card numbers, we might easily overlook corporate trade secrets or competitive data. There's a long list of information that can be considered trade secrets or competitive data. The list for your company will be very specific to the business you're in. We've included a generic list to help prompt your own investigation of data that could be considered confidential to your company. These include:

- Customer or employee databases (used to steal customers or employees)
- E-mails among employees discussing confidential matters
- E-mails among executives discussing company secrets, financial status, or future plans
- Competitive information
- Formulas for products and descriptions of soon-to-be released products
- Design specifications, engineering specifications, and technical diagrams or drawings for current or new products
- Confidential reports, audits, or memoranda
- Personnel files, performance reviews, pay rates
- Financial reports
- Source code for software projects
- Marketing or technical project plans

Unfortunately, due to the variety of data listed here, it's often difficult to definitively point to one or two network locations where this type of sensitive information exists. Usually, it's spread across the enterprise in department-level folders, on e-mail servers, and on individual desktops and laptops. As part of your corporate IT security planning process, you may decide to designate specific locations for this type of sensitive data, to be sure it's properly backed up on a regular basis, and so that you can control, monitor, and audit access to these files. In addition, pay special attention to executives and others who might have access to sensitive information and who travel with laptops. There have been several well-known cases of laptops with confidential or sensitive data being stolen from hotel rooms, locked cars, and airports. In some cases, the thief is just after the laptop. In worst case scenarios, these thefts constitute industrial espionage and are intended to garner trade secrets from a competitor or to steal plans, information, or other sensitive data.

Malicious Data Insertion

Malicious data insertion is a huge problem that is on the rise. Part of the reason is the increase in Internet usage and in the collaboration of malicious software (malware) writers. Hackers are getting along well these days, working together to create bigger corporate security headaches. Malicious data insertion is a risk to every computer on the planet, save those that (for some reason) are completely isolated from the Internet. The risk to individual user computers is clear: malware can steal user names and passwords, track where you go on the Internet, capture your instant messaging, and copy your e-mail. Pretty scary stuff. In the corporate environment, that problem is multiplied by the number of hours the average user is on the network, the type of data carried on the corporate network, and the number of potential "back doors" available to hackers.

Rootkits are one of the most malicious and growing forms of malicious data insertion (see the following sidebar), but they're not the only problems. Viruses, worms, corrupted or modified data, illegal, illicit, or unethical data can all be inserted into your network. We often think of security as preventing unwanted intrusion, which it is, but we sometimes forget that when the bad guys get in, they often want to leave something on your computer so they can continue to siphon data.

In addition, this malicious code can cause computers to become unstable which can result in thousands of lost hours and dollars trying to recover from these incidents. Some viruses or malware are intended to do nothing more than cause the computer to run slowly, generate errors, become unstable, or simply not boot.

Malicious data can also involve inserting bad, erroneous, or illegal data into the company's network. Think about the last time you shopped online: almost every online store uses some sort of database to present product information, including product name, description, specifications, and price. What if a hacker inserted data into that database so that the pricing was wrong, or a competitor's products were displayed, or the company's President's social security number was displayed instead of the product number? In some cases, hackers are pulling a prank; in others, they want to create serious problems and may specifically target a company they want to disrupt.

Business Intelligence…

Malware Threat Rises

An article written by Matt Hines in an April 2006 issue of eWeek.com is titled *Rootkits, Smarter Hackers Pose Growing Security Threats*. The article points to a study released by anti-virus maker, McAfee, on the growing sophistication of hackers and malware writers. According to the article, "Factoring into the issue, and the continued maturation of malicious attacks on enterprise systems, is the growing tendency toward collaboration among hackers." McAfee said its research indicates that the use of so-called 'stealth technologies' has jumped by over 600 percent during the last three years."

If you're not already aware, a rootkit is a set of software tools typically used by an attacker to hide unauthorized activity on the computer, and to evade anti-virus program detection. The tools are intended to conceal processes, files, or data running on the computer in order to evade detection. The issue made headlines in 2005, when Sony BMG music CDs placed a rootkit on Microsoft computers in order to prevent CD copying.

A recent report by Microsoft, the biggest target for hackers, announced it was practically impossible in some cases to get rid of a rootkit. In a separate eWeek.com article, Ryan Naraine reported that Mike Danseglio, program manager in the Security Solutions group at Microsoft, stated at a presentation at the InfoSec World conference that, "When you are dealing with rootkits and some advanced spyware programs, the only solution is to rebuild from scratch. In some cases, there really is no way to recover without nuking the systems from orbit." In fact, when a branch of the U.S. government discovered over 2,000 user computers infected with a rootkit, it had no viable way to quickly scrub those systems and reinstall the operating system.

Continued

As malware threats rise, it's even more important to train users, lock down systems, and have a solid plan in place for wiping out systems and starting from scratch if malware can't be removed in any other way. Be sure your audit looks for these problems as part of your project plan, and as part of your ongoing security operations. (See http://www.eweek.com/article2/0,1895,1949650,00.asp, http://www.eweek.com/article2/0,1895,1945782,00.asp.)

Equipment Theft or Damage

The threat of equipment theft or damage should be carefully assessed and is typically addressed through physical security planning; how buildings, offices, servers, and other network resources are physically secured. Obviously, some items are easier to steal or break than others. It's pretty hard to sneak out of a building with a desktop computer under your coat, but a blade server, router, or laptop is much easier. Your threat assessment should include taking a look at your physical premises to determine how easy (or hard) it would be for someone (insider or outsider) to steal or damage equipment. Network, communication, Web, database, and application servers would be at the top of the list and should be physically secured. Beyond servers, there are plenty of network resources that, if stolen or damaged, could hinder or halt business operations. Items such as routers, gateways, hardware firewalls, and network storage devices are critical to daily operations, and should be included in your physical security assessment.

Risk Assessment: Legal Liabilities

You may need executive or legal input to understand the company's legal liabilities, so make sure you have the right people involved in this assessment. For example: A specialty food distribution company sells to other businesses and directly to consumers through an online Web store. The company carries an inventory of about 5,000 products and its product catalog is available online. It keeps track of various data (e.g., business customers' purchase orders, order history, returns, and so forth.; consumer names, addresses, phone numbers, and order history; and vendor order history, stocking levels, pricing, transportation costs, and discounts. It processes credit cards through a third-party credit card processing company, and does not store credit card numbers, expiration dates, or related data. What are the company's legal liabilities? On the vendor side, they're pretty low because the data is probably not very interesting to most hackers (excluding industrial espionage). On the customer side, the business customer's order numbers, order history, and purchase order numbers are also not particularly useful to a hacker, unless someone wants a list of customers. Again, not particularly useful or lucrative data to go after. Finally, the consumer data (e.g., credit card information, expiration dates, names, addresses, phone numbers, and so forth. What's the liability here? If the company has a secure connection to the credit card processing company, and if they never store that data, then the liability is more limited than if they inappropriately store credit card data in order to do a bit of "data mining." However, the security of the transmission between the credit card processing Web site and the company Web site should be assessed, as should the overall security of the Web site itself.

As you can see, by looking at your business processes from the hacker's perspective, you can better determine where your legal liabilities lie and how best to address them. It's important to understand what a hacker might go after and what the legal liabilities are in each of those scenarios. Make sure you also understand what, if any, legal protection your firm has in the event of a breach, and what impact a breach might have on your organization such as blacklisting your domain name due to unauthorized spamming stemming from a breach. Make sure to include your firm's legal representative in this discussion, to make sure you haven't overlooked any legal elements. For a more detailed look at legal liabilities, pick up another Syngress title, *Network Security Evaluation: Using the NSA IEM* (see Chapter 5).

Third-party Attacks

Third party attacks are most common in the wireless arena, where an attacker (usually a spammer) sends unsolicited e-mail via your network connection. It's simple enough once an attacker gains access through an unsecured wireless network connection. In those cases, it is your network's IP address that will be tagged as the source of this spam, even though no one from your company actually sent the e-mail. Many states are instituting legal and financial penalties for spamming, and your company could be found liable for spam it never sent. Beyond the possible legal and financial penalties, your networks' IP address could be blacklisted or shutdown due to this type of activity, unless you have some way of proving you were the victim of a third-party attack. Even then, restoring order and connectivity can be extremely difficult. Another growing and disconcerting kind of attack are zombie nets, which are Distributed Denial of Service (DDOS) attacks.

Illegal Data Insertion

We talked about malicious data insertion, but we didn't specifically discuss the legal liabilities that can come from it (as opposed to malware, rootkits, and so on). There are two ways illegal data ends up on your network. First, stolen content could be placed on your network from an attacker who gains unauthorized access to the network. They may place stolen data there in order to blackmail the company, to embarrass the company, or to get the company in legal hot water. Suppose a hacker (or disgruntled employee) places unlicensed, stolen software on your network and then reports your company to the authorities? Suppose a competitor's blueprints or technical drawings end up on your network and it is somehow discovered? These kinds of activities may not steal your data, but they can certainly disrupt business operations, cost a lot of money, and create significant legal liabilities.

Risk Assessment: Costs

At some point in every project planning process, you should ask the question, "What if we do nothing?" The reason for this is to avoid solving a problem that doesn't need to be solved. In the case of corporate IT security, you shouldn't just "do nothing," but if you start from there and work your way up, you can begin to understand what is required and what might be optional, since you're likely to have to make trade offs at some point.

Once you've decided to implement corporate IT security, you'll need to include the initial and ongoing costs of securing the network to your cost estimates. If you already have an IT security solution installed, you'll have to address the cost of both the ongoing (in place) IT security, and the new security initiatives. Your costs include securing the network data, securing the network connection, securing network communications, and securing end-user devices (laptops, Personal Digital Assistants [PDA's]). You will continually have to balance operational security with operational efficiency and security costs with remediation costs.

In addition to these implementation costs, you need to assess the cost of a network security breach to the organization. If the network is compromised, how much will it cost you to repair the damage? What are the costs of remediation, legal defense, and possibly marketing and public relations to address a potential breach? Finally, you need to look at the cost/benefit analysis to determine how all the potential costs of a breach compare to the cost of securing the network in the first place. Though the answer almost always comes out in favor of pro-active security solutions, you need to be comfortable with your analysis so that you can defend it to your executive team or project sponsor.

People

When performing a risk assessment and looking at costs, you need to start with the people needed to design, implement and maintain security. Without the right people in place, your costs (or schedule) can mushroom and you can still end up with a network full of security holes. Critically assess your team's skill set and be brutally honest with yourself about the skills your team has and the skills it lacks. Hiding your head in the sand won't change the cost of the project but it will change the outcome if you don't have the needed skills. As mentioned earlier, hiring an outside security consultant can be costly but the quality of the result can end up saving you time and money on the other end of the project. If an outside consultant isn't warranted or affordable, you'll need to find alternative ways of gaining the expertise you need at a reduced cost. That might involve training current staff (which still leaves them at the early stage of the learning curve), hire a well-qualified temporary employee (which comes with the danger that he or she will open a back door into your network), or hire a full-time employee with the requisite skills. It's going to cost you no matter which way you approach it, so you might as well find your best alternatives early in the process. It's usually an investment that's well worth it.

Training

As part of your security assessment, you'll need to look at the training needs of the entire organization related to security. As we've stated, security is not a one-time activity; it takes the awareness, attention, and compliance of all network users to help ensure a secure network. As such, there are a variety of training activities that will probably be needed and which should be assessed early in the planning process.

- **Installation and Configuration** Equipment that is improperly installed and configured creates a huge security hole. Think of all the wireless routers out there using the default administrator username and password. IT staff may require vendor-specific training on equipment, especially servers, routers, and firewalls, among others. Remember that training provides the necessary knowledge to IT staff, but there's no substitute for hands-on experience.
- **Network Operations Training** The ongoing operations of the network is where security is monitored, maintained, and managed once the security plans have been implemented. Therefore, as part of the assessment, it's important to begin identifying what ongoing operations are required to maintain security once it's established. It's important for those responsible for managing the day-to-day network operations to be well-versed in secure operations, and to be well-trained in operational issues. Whenever pos-

sible, send your employees to vendor-sponsored training on the equipment you use. It's a great way to ensure your employees are well-trained on network equipment, and a great way for your employees to learn about the latest tips, trick, and threats from the instructor or other class participants.

- **End-user Training** End-user training is often overlooked in the security planning process, yet we all know that users can be the first line of defense. When users understand the threats that exist, they can actively participate in keeping the network secure. For instance, if employees understand that downloading files from unknown sources (and some known sources) can result in malware being installed, they tend to be a bit more cautious about downloads. If they understand that an unusually slow computer or altered files can be a sign of virus, worm, or malware infection, they can quickly report it rather than disregard it. Also keep in mind that each company should have policies in place regarding safe and approved computer behavior. Each employee should be trained in these policies and ideally should have to acknowledge, in writing, that they will comply with these policies. While training can be a significant expense, the upside is that properly trained users are less likely to put the network or the company's data at risk. We know the cost of remediation is very high both in real dollar costs and in lost productivity. The cost of training is almost always offset by the real reduction in security risks.

Equipment

When performing a risk assessment and looking at costs, it's important to include equipment—both equipment that needs to be protected and equipment that protects the network. Equipment that needs to be protected are all network servers, routers, switches, hubs, firewalls, desktops and mobile devices (your list might be longer). These devices need to be physically protected from theft, damage or unauthorized use. In addition, these devices need to be protected from remote attack such as data insertion, data manipulation, or data theft. On the other side of the spectrum is the equipment you use to protect your network, including firewalls, isolated network segments (and the equipment used to create those subnets), routers, and more.

Sometimes it's helpful to look at what network level (data link, network, application, and so forth) your equipment is operating and how it needs to be protected. In other cases, it might be more helpful to look at your network map and determine where security is needed.

Regardless of the security solution you're working on (corporate IT security or one of the individual security area plans), you're probably going to have to buy software or hardware to complement your security efforts. You can harden your servers, disable unused TCP/IP ports, set up auditing, and tighten access controls but you still need firewalls, anti-virus, anti-spyware, and other security systems to complement those efforts. Again, be sure you do a thorough inventory and assessment before sitting through any company's sales presentations. Define your goals, your needs, and your parameters first, then sit through the presentations. Companies will almost always try to up-sell you. Sometimes that's a good thing because they add value to the process; however, other times it's just about making more money. If you are clear about the equipment and the solutions you need before you sit down and talk with anyone, you're more likely to purchase just the solutions you need, not the ones the company wants to sell you.

Time

When IT staff members are on salary, there's a tendency to forget that time is money. IT security can take up tremendous amounts of time in many different areas, and the risk assessment and the associated costs should include the cost of people's time. When planning the time for the risk assessment and the security plan implementation, include tasks such as:

- Equipment specification development
- Equipment purchase (direct purchase or through a bid process such as Request for Quote [RFQ])

- Equipment set up, staging, testing, configuration, and installation
- Integrating security solutions into existing infrastructure (planning, staging, testing, implementing)
- Maintenance, operations, and recovery procedures
- Baseline testing and documentation
- Security policies and procedures
- Vendor contract negotiation and contract management

Time is a cost that should be captured within your assessment and in your project plan. When you delineate your project's tasks, you'll capture the estimated duration (how long you'll allow for the task to be completed) so you can create a project schedule. Depending on how your company works, you may also be required to capture labor costs. In these cases, you'll need to estimate the time (effort) it will take to complete a task, and calculate the labor cost based on the wages of those who will be completing the task. Add tasks like those in the above bulleted list, so that you don't inadvertently underestimate your labor costs in both the assessment and project implementation phases.

Impact Analysis

How much would it cost your business to be down for one hour? One day? One week? As part of your risk assessment, you need to identify your critical business systems and processes that most impact your business revenues, your assets, and your clients or customers. These should be ranked in order of direct and indirect costs. It's not enough to merely determine that you'd lose $54,000 per hour of revenue. What is the cost in terms of lost productivity, IT staff time spent on remediation, employees unable to access critical data, and the press getting wind of your security breach? Identify your business systems, evaluate the impact of an outage, and prioritize them so you can focus your attention on addressing the most critical aspects first. You can use a model like the one shown earlier (in Figure 10.1) as an aid in defining your impact analysis.

Since you're likely to implement your security plan as a corporate IT security plan with smaller individual plans incorporated, you can choose to implement the most critical ISAPs first. This reduces your security risks quickly while providing a comprehensive approach to corporate security. As we've discussed throughout this chapter, the potential impact goes far beyond the financial impact and can include:

- Immediate financial loss
- Long-term financial loss
- Loss of customer confidence
- Industry or market loss of confidence
- Bad press or intensive press scrutiny/investigation
- Regulatory, statutory, or legal investigation
- Shareholder scrutiny or lawsuits

There are companies that perform impact analysis as part of their consulting services, but in many cases, you can perform this assessment yourself or with help from key members of your company. The analysis should include identifying the most critical business processes across your entire company (not just the headquarters or location you're most familiar with). After identifying these critical business processes, you should identify the maximum outage your company can afford to sustain before it severely impacts the well-being of the company. According to the Gartner Group, 50 percent of all businesses that suffer a data loss due to attack or system failure went out of business within three years of the attack if they failed to restore the lost data within 24 hours. Your impact analysis should include the impact of both a full and partial outage. Your recovery and remediation plans should also be well-documented, so that you are able to recover quickly. Your impact analysis should address the financial, productivity, and personnel impact of an outage, and you will also need to account for the potential legal liability (and the related financial impact of legal defense and litigation) of a security breach that exposes confidential or personal information.

The impact analysis should also take into account the priority of recovery. Clearly, when a security breach is discovered, the first priority it to close the gap and secure the network. Once that is accomplished, however, additional work must be done to assess the scope, nature, and impact of the breach. Recovery and remediation plans should be prioritized based on business impact, so that the most important systems are brought back online as quickly as possible. Sometimes in the heat of the moment, people tend to go after the "low hanging fruit" and focus on the tasks that are easiest or fastest to accomplish. Having an impact analysis and prioritized list at your disposal during these crises can help you focus on getting the most important work done first without having to try to evaluate priorities during an "emergency."

Public Access Networks

One of the most neglected areas is that of public access security and the impact to business via a breach in this arena. Here's the most common scenario: A busy VP of Marketing is traveling to an important client meeting. She's waiting in an airport for her flight and is waiting for one of her staff to make a key revision in the presentation she's making at the client site. She fires up her laptop and checks her e-mail. While online, she opens another document, makes a few changes, and saves it. She logs off, saves the updated presentation to her laptop, turns off the computer, and boards her plane. It all sounds innocent enough until she checks into her hotel room and fires up the laptop. Now she finds that she can't logon to her e-mail account. She gets a message saying username or password is invalid. She contacts the IT help desk but it's after hours and she gets a recording and the option to page someone. She's very tired, it's been a long day so she lets it go until morning. What she doesn't know is that sitting in the airport was someone just waiting for someone else (the VP of Marketing in this case) to log onto an unsecured wireless network that appeared to be the airport network. The bad guy now has her corporate username and password, which happens to be the same for her e-mail. The bad guy now has access to everything on her corporate network, and he's been reading her e-mail while she is in meetings.

Because she's a fairly high level corporate employee, chances are good her user account has permission to access highly confidential material. Certainly she (and now the bad guy) have access to marketing plans and projections, financials, and more.

Most IT staff will focus intently on the impact to business operations if the corporate network is attacked directly, but the scenario described is becoming more commonplace. When looking at the potential impact, look at all of the ways your company's employees connect to corporate data and look at the potential impact of these means of access.

Legal Implications

We discussed the legal implications at great length, so we won't repeat that here other than to say that it should be abundantly clear to you by now that there are significant legal aspects to IT security that must be assessed and addressed in a clear, thoughtful, and intelligent way. The future of your company literally depends on how well you do your job in this area. No pressure.

After performing a thorough risk assessment, audit, and/or impact analysis, you should have a very clear idea of what needs to be secured and what the priorities are. When you looked at the impact of systems outages to your business, you should have developed a prioritized list that would help you in two ways: you know what you need to secure first, and you know where you need to focus your IT resources, including your staff, your budget, and your project planning efforts. You can prioritize your ISAPs based on this analysis and build them into your corporate IT security plan in a phased manner. This helps by reducing the project scope, schedule, and budget and allows you to focus completely on one particular security area at a time. Granted, not everyone can implement security solutions in a sequential manner, in some cases you'll have to run security projects in parallel. We also recognize you don't have the luxury of just running a security project. IT staff have multiple ongoing responsibilities on a daily, weekly, and monthly basis. The security project will be "just another task" on the long to-do list for many. Breaking your corporate IT security project plan down into smaller s can help staff focus on the tasks at hand without overwhelming them with a massive corporate security plan.

Thus far in this chapter, we've talked about your risk assessment and impact analysis. We've gone into great detail, but you can dig even deeper. This should provide you with an excellent framework for understanding your corporate IT security needs. As we mentioned, you will have to circle back through this more than once, because the corporate IT security plan depends on a full assessment. Regardless of your approach, you will want to revisit your data at least once and refine it as you go, to make sure your corporate IT security plan is as comprehensive as possible. Remember, there is no perfect security solution and you can far outspend your need for security; thus, striking a balance should be your goal. Next, we discuss the parameters for your corporate IT security plan.

Business Intelligence…

Scan the Headlines to Avoid Common Mistakes

We all have those "duh" moments when we realize we've made an incredibly dumb mistake by overlooking the obvious. One way to avoid common security mistakes is to scan the headlines for what's happening in the rest of the world. Many IT professionals subscribe to a variety of online newsletters including security-related newsletters, which is one way to stay on top of changes in the world. In addition, scan newspaper and magazine headlines on a regular basis. If possible, include a "what's new in the world of security" segment in your IT staff meetings, and assign one or more people each week to come prepared with a five minute presentation (sans PowerPoint) on a security-related topic. Look at the problem, how it was detected, and how it was corrected. This information can be extremely useful in detecting and avoiding security problems internally. It keeps you and your staff up-to-date, sharpens your skills, and can also make for very interesting staff meetings. And, chances are if they were exploited elsewhere, they'll be exploited in your organization before long.

Authentication

Authentication is the process of verifying the identity of any entity requesting access to network resources. Authentication encompasses server and host authentication, router or wireless access point authentication (where applicable), process authentication, and user authentication.

Authentication and authorization are not exactly the same thing, though in some cases such as legal or technical requirements, they are often paired or confused with each other. However, authentication is the process of making sure you are who you say you are, and authorization allows access based on that identity.

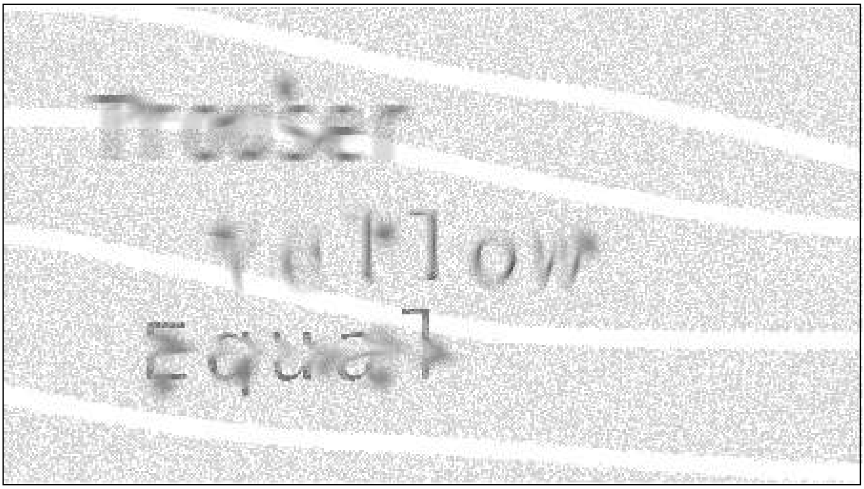
Your project plan should dig into your authentication security to determine how effectively you've implemented authentication systems, where your vulnerabilities lie, where and how an attacker might strike, and what you need to do to improve security. While ever-changing, the list presented here shouldn't change too dramatically in the near-term, unless some major event or discovery obliterates previous authentication solutions.

- **Basic Authentication** Users signing into a guest account have to know the guest account name and password.
- **Two-factor Authentication** The username and password are two factors required to log onto a network. This is similar to entering a credit card number and the expiration date for an online transaction.
- **Multi-factor Authentication** The username, password, and pin number are all part of multi-factor authentication. Many banks use multi-factor authentication to prevent theft based on URL spoofing. Multi-factor authentication includes entering a user name and then being presented with a unique key such as a picture or key word, and then entering your password only after the correct key is presented to you. This prevents specific types of attacks, such as man-in-the-middle (MITM) attacks.

- **Public Key Infrastructure (PKI)** PKI is a form of cryptography that is implemented as part of a security project. PKI allows users to communicate securely through the use of a pair of cryptographic keys. One of the keys is the "public" key and one is the "private" key, and they are related to one another mathematically.
- **Geo-location** Geo-location is a method of determining where in the world a particular computer resides. It's used for a number of legitimate purposes, but it can also be used for illegitimate purposes. Many companies sell IP address geo-location databases that can locate the city and the street Justas well as the country of an IP address. Anonymous traffic can help deter geo-location efforts, but many Internet companies will not accept or forward anonymous traffic.
- **Kerberos** An Internet security protocol that prevents eavesdropping and replay attacks, and ensures the integrity of the data. It is implemented between clients and servers and provides mutual authentication.
- **Secure Shell (SSH)** SSH is one implementation of public key cryptography that provides for mutual authentication of user to a remote server. It also provides data confidentiality and integrity.
- **Secure Remote Password (SRP) Protocol** The Secure Remote Password Protocol is a password-authentication system that allows users to authenticate with a server. This method is resistant to dictionary attacks and does not require a trusted third party.
- **Closed-loop Authentication** Closed loop authentication is a means by which one party verifies him or herself to another party by requiring the use of a token transmitted from a trusted point of contact.

- **Remote Authentication Dial-In User Service (RADIUS)** RADIUS is a protocol that provides authentication, authorization, and accounting (AAA) for network access and mobility. It works in both local and roaming situations.
- **DIAMETER** DIAMETER is an AAA protocol that is purported to be the "upgrade" to RADIUS, although it is not backward compatible.
- **Hashed Message Authentication Code (HMAC)** HMAC is a type of message authentication code that uses a cryptographic hash function in combination with a secret key.
- **Extensible Authentication Protocol (EAP)** EAP is a fairly universal authentication mechanism that is often used to secure wireless networks and point-to-point connections. There are variations of the EAP protocol that are incorporated into recent Wireless Protected Access (WPA) and Wi-Fi Protected Access 2 (WPA2) standards for wireless networking security.
- **Biometrics** Biometrics are used in computer security through fingerprint, retinal, and facial recognition, among others. Recent studies have shown that some of these methods are easily spoofed.
- **Completely Automated Public Turning Test to Tell Computers and Humans Apart (CAPTCHA)** You may have run into this type of authentication without knowing its name. It's used to tell humans apart from machines by preventing automated responses. It falls into the category of challenge-response authentication. Typically, a word or set of numbers and letters are presented that are obscured or modified in some manner to prevent computers from responding to a prompt. Figure 10.2 shows an example of a CAPTCHA.

Figure 10.2 Sample of CAPTCHA Used to Prevent Automated Responses



Authentication can be accomplished in a number of ways. This section is not meant to teach you about authentication as much as it is meant to get you thinking about the kinds of authentication you may have or may want to research as you begin developing your IT security project plan. We discuss cryptography in a later chapter, with an eye toward developing individual security area project plans.

Business Intelligence…

CAPTCHA

You may not need to know about CAPTCHA to develop your authentication and authorization assessments, audits, and recommendations, but it's a very interesting concept that's worth knowing about. This is one of those areas that you'll learn about sooner or later if you have your staff actively looking for innovations in the security world. Developed by the brilliant folks at the School of Computer Science at Carnegie Mellon University, the CAPTCHA can be used in a variety of applications, among them thwarting automated responses. There are several iterations of this method. The most basic is called "Gimpy," which distorts text so that

Continued

human eyes can still recognize and read the text, but computers cannot use automated programs to discern the letters in the text image. "Bongo" is a system where the user is shown visual images and asked to determine where a third image should be placed. "Pix" relies on a large database of labeled images. The database then pulls four (or some number) of related images together and asks the user to identify the unifying element (e.g., it might show a picture of a lake, an ocean, a sailboat, and a glass of water). The unifying element can be selected from a long list that includes the word "water." CAPTCHA uses a sound file to say or spell a word, and then the listener must type in the word he or she heard.

CAPTCHA's are good for a lot of things, but keep in mind that they're not friendly to those who have sight or hearing problems (e.g., visually impaired people often use screen readers to determine what's on their computer screen. Clearly, visually based CAPTCHA's can be problematic, because aurally based CAPTCHA's would exclude people who are hearing impaired. While this may be a small portion of your population, it is something to consider before implementing this type of system. For more information on CAPTCHA, go to www.captcha.net.

Access Control

Access control can be thought of as authorization and encompasses three areas: physical access to equipment, local access to the network, and remote access to network resources through Virtual Private Network (VPN), the Internet, or wireless connections. As shown earlier in Figure 10.1, the layered approach might help you visualize your network and look at access control from that perspective (e.g., how do you physically control, monitor, and detect a breaches access to the elements defined? How do you virtually control, monitor, and detect breaches to access?

Physical Access to Equipment

As part of your ISAP, you need to assess and audit the physical access to your equipment, and devise strategies for improving that aspect of security based on the results of your assessment, testing, and auditing. Restricting and monitoring access to key network components such as servers and routers, is an important part of securing the network that should be addressed in your security project plan. Obviously, there are limits to how secure you should make equipment. Users need access to some of the network resources, including desktops, laptops, PDAs, and other wireless devices. These assets should be protected to the greatest extent possible to prevent an unauthorized person from using or stealing the equipment (e.g., What happens when the receptionist steps away from his or her desk? Is the front door locked? Is there a security person or camera? Does your company's security policy dictate that he or she lock his workstation first?). Also, compliance issues such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA) can come into play. What if the receptionist who leaves the desk unattended works in a doctor's office or a hospital emergency room? In that case, you have two issues—the security risk and the HIPAA risk.

Local Access to Network

Local access is typically controlled through username login requirements, although as mentioned in the previous section, it is also tied to actual physical access to the system. Look for ways that unauthorized persons might gain access to the local network. This is clearly the largest area, because we have to include usernames, passwords, access control lists, security and user groups, permissions, and how they replicate throughout the organization. These areas should be reviewed and addressed as part of your assessment and included as discrete tasks in your security project plan. Local access can also include someone slipping a wireless access point onto a network node that is hidden or in an obscured location.

Remote Access to Network

Remote access includes access to the corporate network by employees physically located outside your network, as well as other connecting points into the network such as extranets and Web sites—anyplace that the inside and outside come together. An attacker would prefer to sit in the comfort of home to wander undetected through your network, so all external-facing access points must be assessed and addressed in your project plan.

Auditing

Different people view auditing in different ways, but the net result is that auditing should examine and expose any shortcomings of IT and company security policies in a systematic manner. The challenge for many IT departments is twofold. First, policies almost always come from outside the IT department, so you have to actively advocate for policy change and work collaboratively on a cross-functional team to accomplish this goal. For many in IT, that's not an appealing proposition. Second, developing policies and procedures based on the outcome of your auditing, is a task that requires less technical ability and more organizational agility, which are two primary reasons why IT audit results sometimes don't make their way back into organizational policies and procedures.

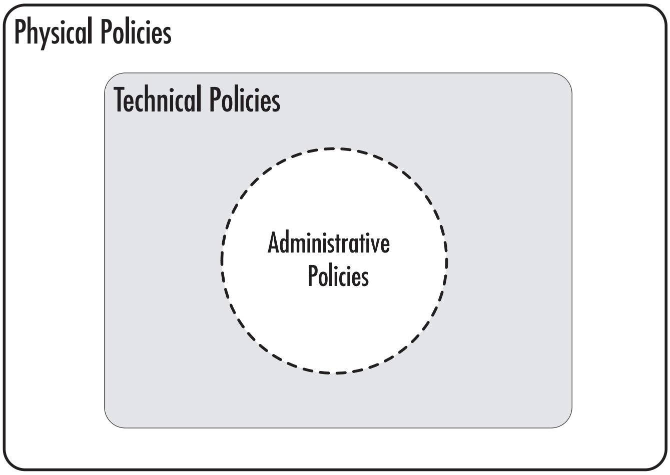
Many IT security experts agree there are five major components of a security audit: policy review, process and procedure review, operational review, legal requirements, and reporting requirements. Let's look at each of these areas in more detail so you can include tasks in your IT security project plan to address these components.

Policy Review

There are all kinds of corporate policies that directly and indirectly impact network security. This is an area that you should have representatives from different areas of your company provide input. At minimum, you should have one or more representatives from Human Resources to provide guidance on current policies, how suggested changes to policies might be implemented, and whether there are any legal or Human Resources considerations for such policy changes.

There are three basic kinds of policies, as shown in Figure 10.3. The physical policies truly govern who can physically access equipment, including servers and other mission critical components. Technical policies govern who can do what with a network resource. Technical policies are often governed by or created from administrative policies, the third piece of this puzzle, which outline how corporate resources are used.

Figure 10.3 Three Layers of Security-related Policies



Physical

Physical policies prevent unauthorized access to network resources, which basically prevents theft and tampering on a physical level. Physical policies are often dictated by administrative policies (e.g., you might have an administrative policy that says that only senior IT staff have access to server rooms. You might enforce that policy through physical policies such as installing a card key system that only senior IT staff identification (ID) cards can open, or using a keypad with unique Personal Identification Number (PIN) numbers for each senior IT staff member. While these are clearly physical barriers to entry, they also reflect or enforce administrative policies through technical policies (which card keys or PINs are authorized). Notice that these three areas are always intertwined.

Technical

Technical policies are enforced by the operating system or other related technology, not by physical means. A technical policy addresses various technical requirements such as the requirement to use strong passwords or a policy regarding how confidential data is encrypted. These technical policies are, in a sense, the second line of defense after physical policies. However, since attackers often don't require physical access to the network, physical policies are inadequate by themselves.

In addition, technical policies that should be audited include the full scope of how users access the network and what methods are in place to monitor network activities (e.g., how user groups are created and maintained, how it is determined which user gets membership to which groups, how group permissions are assigned and replicated through the enterprise, the administrative procedures for maintaining appropriate group permissions, and related activities).

When we talk about auditing, we're talking about looking at the security environment, but there is also the discrete activity of auditing that involves tracking various network events through the use of log files and alerts. What you audit is strictly dependent on your unique network environment. If you audit too many events that don't directly help you manage security (or other critical network aspects), you risk becoming bogged down in mundane log files and non-critical event evaluation. If you audit too few events, you may miss seeing a pattern of repeated attack or inquiry (perhaps an attacker is gathering information and has not yet performed an intrusive attack). In this case, auditing is part science and part art. You have to carefully determine which events are worth auditing, understand what the audited event will actually tell you about your network activity, and create a process for routinely reviewing log files. A log file containing all the clues to an imminent network attack is useless if no one ever looks through it and analyzes the logged events.

Providing a full list of auditable activities is outside the scope of this chapter, but there are great resources available to help you develop a meaningful network auditing process so that you can be sure you're looking at log files and audit files that help you maintain security across the enterprise. To get you started thinking about log files and auditable events, we've created this high level list for you:

- IDS logs and session logging
- Firewall reporting
- Systems and network reporting
- Report management (what needs to be reported to whom and how files are managed)
- Managing log files with a log parser

Business Intelligence…

Buried by Log Files

You've undoubtedly had a lot of experience with log files. You know that you can set auditing requirements in just about any way you want, and at the end of the day, those audit activities create alerts and log files. While there are automated ways of reviewing log files, they're not without flaws. Being overrun with data is not helpful if you can't discern the potentially important events from normal daily network activities. As Jacob Babbin puts it, it's really about "identifying the patterns in the chaos." (*Security Log Management*, Jacob Babbin, Syngress Publishing, Inc., 2006). Jacob (and others) put together a great resource to help you figure out what you need to log, what you need to do with those logs, and ultimately, how you can see "the forest through the trees" when you're managing security logs in the enterprise. You can also find articles specific to managing log files in the Windows environment on the Microsoft Web site at www.microsoft.com/technet. When all is said and done, it's your job to determine which events to audit and to manage log files in a manner that enhances and maintains security. A log file that isn't read and acted on is just a waste of 1s and 0s on your network storage device.

Administrative

A variety of administrative policies are required to describe in detail how security is maintained. These run the gamut from policies regarding which level of access a manager is granted, which employees should be granted remote access capabilities, and how passwords should be created, secured, and maintained. Policies regarding the use of the Internet, the ability to download from the Internet, or the ability to install new programs fall under both administrative and technical policies. The administrative policy describes what is and is not allowed and technical policies are created to enforce those administrative policies. This can include blocking certain Internet sites and disabling the feature that allows users to install new programs and other technical safeguards. Administrative policies are typically included in employee handbooks, reviewed during employee orientation or awareness campaigns, and maintained through active management.

Administrative policies also help define the culture and attitudes toward security within an organization. While some companies go a little crazy with policies and procedures, others are far too lax. You'll need to work with key stakeholders in your organization to find the right balance between securing the network and over-burdening management with policies that are unenforceable or unmanageable.

Process and Procedure Review

Here is another area in which you should have strong Human Resources input, because many of the security processes and procedures are directly related to personnel management (e.g., what happens when an employee is hired or fired?). In some organizations, it can be days before a fired employee's account is disabled. A policy that states that the account of any terminated employee should be disabled within ten minutes of termination should then be coupled with a process for doing so. This might involve having the firing manager or Human Resources notify IT through a defined process so that the account is quickly disabled. What about when a new employee is hired? Are there any policies regarding background checks for employees working in Human Resources, IT, or finance? If so, you also need to have a process for making sure the background check is performed.

Operational Review

Your operational review should accomplish the following:

- How consistently are the policies and procedures related to security applied and enforced?
- How do day-to-day operations enhance or degrade IT security?
- What operational plans are in place to address security in the various areas? Ideally, each area should be assessed individually and as part of a holistic system.

Your operational audit should look at four discrete elements that help build a secure framework. First, you should provide the least privilege necessary for any user to perform the functions of their job. Second, you should reduce the attack footprint by disabling, removing, and uninstalling anything on the system that is unused, including equipment, modems, ports, software packages, protocols, and the like. You should also look at the various security layers, sometimes called *depth-of-defense*, to ensure your policies, procedures, and operations support your security objectives. Finally, you should work diligently to identify the inherent assumptions you're making about your network, your users, and potential attackers (people, process, and technology assumptions).

Legal and Reporting Requirements

Although listed last, it might actually be the first task, chronologically, that you perform in your audit function because it often helps to know what your legal requirements are for your audit. If you must conform to various government or legislative regulations, you should state these at the outset of your audit process. As part of your project plan, you should have defined your various requirements and all legal requirements should be listed. This will help you devise an audit plan that ensures you meet these requirements. In addition, you may have legal or corporate reporting requirements. Again, these should be defined at the outset so that your audit is conducted in a manner that facilitates the required reporting. For example, you may need to collect a particular type of data that can only be collected at the time the activity occurs. Therefore, your audit requirements should list this and these requirements should be built into your task's completion criteria.

Attacks

Attacks come in all shapes and sizes, and the list of common attacks provided here will no doubt change before the ink on the page has dried. Still, old habits die hard and some of the most common attacks have been around for a long time. In this section, we provide a list of attacks to look for, to prompt you to think along these lines. However, be sure to sit down with your team and research the latest attack methods as well as the best practices for addressing these attacks.

Attacks can generally be categorized as *intrusive* and *non-intrusive*. Intrusive attacks include password attacks, DOS attacks, network sniffing, spoofing, session hijacking, and application and database attacks. Non-intrusive attacks include network and host discovery (using a variety of techniques), port scanning, war driving (and related activities), and information reconnaissance. Intrusive attacks usually cause damage; non-intrusive attacks are typically the precursor to intrusive attacks, because they involve gathering information about their target prior to the actual attack. Therefore, let's start by talking about various non-intrusive attacks that provide vital information to an attacker in preparation for the actual assault.

Non-intrusive Attacks

Non-intrusive attacks are intended to gather information typically needed to perform an intrusive attack. There are various kinds of non-intrusive attacks; the following list is just a sampling. You need to look at all the different ways your network can be evaluated or sized up by the bad guys, so you can determine how a non-intrusive attack would generate needed data for a later, more invasive attack. Let's look at a few of the more commonly used non-intrusive attacks and how they should be incorporated into your own assessment, testing, and audit plans.

Information Gathering

We previously discussed various kinds of data that hackers try to access, including user account information, contact names, e-mail addresses, and phone numbers, as well as system configuration data and external connection data (extranets, phone lines, and so forth) This type of non-intrusive attack is called information gathering (also known as *information reconnaissance*), because the attacker is simply gathering data from public or easily available sources. While you can't prevent this information from being gathered, you can think of ways to reduce the value of this data, such as using generic e-mail addresses for public use. Your audit activities should include an examination of all of the public data you can find on your company (e.g., phone book, Web site, search engine, public records, domain name registration, and so forth), and ensure it is as minimal and generic as possible.

Server and Host Discovery

Finding the addresses of key servers is one of the goals of most hackers. There are two distinct ways to accomplish this task. One is to access the network and start "taking inventory." The other is to find a source that will tell you everything you need to know. One of those sources is the Domain Name Server (DNS) directory, that will give you all kinds of information about the structure of the network. The variety of record types used in the DNS can yield a wealth of hacker-friendly information. A thorough discussion of DNS is far outside the scope of this book, but it is an area your IT security project plan should incorporate. Active Directory (in the Microsoft world) and other directory services are also potential gold mines for attackers.

Aside from DNS and other directory services, there are many other kinds of information about your server and hosts that a hacker would love to get their hands on. This includes all network configurations, system components (routers, switches, hubs, and so forth), wireless networks, telephony equipment and configuration data, power and control systems for your network, and other data that generally cannot be enumerated via a directory scan.

Your audit should perform the same kinds of enumeration and discovery techniques that a hacker would use to try to determine the configuration and layout of your network. There are numerous techniques and tools you can use for this set of tasks.

War Dialing and War Driving

War driving (also known as *war dialing*) is when an attacker drives around looking for open wireless networks. Many organizations have dial-in connections to their networks that are no longer used but still active, or that are active but not secured. It's easy to dial phone numbers during off-hours to try to find a modem that automatically throws handshakes at you. Your audit should identify all existing modems and the current state of the security on those lines.

Port Scans

Another non-intrusive attack is a *port scan*. When an attacker is looking for a way in to your network, he or she may perform an initial port scan to see what ports are sitting open for them to enter through. The TCP and the User Datagram Protocol (UDP) both use ports to identify session and services information, and to transmit this data back and forth among machines using these protocols. Ports should be scanned on your end, and your security project plan should include ports that are listening, filtered, and closed.

Intrusive Attacks

Intrusive attacks intrude into your network for a definite purpose. Once an attacker has gathered data using non-intrusive techniques, he or she now have the needed data to actually get into the network and do some damage. Two major objectives for hackers are to get in and out quickly, and to do so in an undetected manner. Therefore, your job is to make it hard to get in and out, and even harder to do so without detection. It's a never-ending high stakes game of "cat and mouse." Let's look at some of the intrusive attack techniques you should include in your network security assessment and audit.

Password Attacks

Password attacks are the easiest and most commonly used intrusive attacks. They can be done through social engineering (e.g., "Hey, Jake, I forgot the password for the database, can you e-mail it to me? I'm working from home today. Thanks!"), brute-force attacks, dictionary attacks, and password capture.

DoS

Traditional DoS attacks flood Web servers with so many packets, that it is forced to deny service to legitimate users. This was a very popular attack style about ten years ago but is still used in a variety of less-well known ways. A DoS can happen at a Web or Internet connection point or at a server, where the CPU is overloaded with bogus requests it must respond to, thus forcing out any legitimate CPU requests. A new variation, DDoS, gained favor among hackers in the recent past.

Network Sniffing

Network sniffing is the process of capturing and examining network packets to gather information to be used in an attack. Your assessment and testing should include network sniffing, but keep in mind that sniffing must be done on the local network. That means that you can't do it remotely. Your policies, procedures, and technology should help ensure that sniffers are not used on your network; however, there is no danger of remote sniffers. Also keep in mind that switches, which are "smarter" than hubs, are designed to send traffic to one specific host instead of broadcasting to everyone on the segment. As a result, switches are vulnerable to network sniffing attacks and should be tested in your organization.

Spoofing

The three most common kinds of spoofing are DNS, e-mail, and IP. Each type of spoofing attempts to impersonate legitimate network or electronic traffic in order to gain access to valuable data. Your assessment and testing plans should include tests to see how easily (or not) spoofing can be used on your network.

Session Hijacking

As you know, a session is a specific connection between two computers. Sessions are created in order to exchange information between hosts on a network. If a session can be hijacked, a hacker can insert his or her computer into the exchange and gather information. Sessions can be hijacked at the application level, the host level, or the network level. Your assessment and testing should include a determination as to whether your network uses transport protocols that are unencrypted (which could lead to session hijacking vulnerabilities), if you have ports that could be easily hijacked, or if you have applications that have been written with security in mind (terminating idle sessions, testing user input, use digital signatures, and so on).

Application Attack

Commonly used application attacks that have received a fair amount of publicity include buffer overruns (stack and heap) and integer overflows. Assessment and testing plans should address these issues.

Database Attack

Database management and the attendant requirements for security can fill volumes on their own. Databases are becoming more complex and securing them is becoming more difficult. Ironically, even today, many databases are the weakest link in the security chain. Database servers should be tested for proper configuration, all updates and patches should be applied, and access should be strictly controlled. Scripts should be tested to ensure that errors that can be forced (or are accidentally generated) do not compromise the security of the database server or the database itself.

Assessment and Audit Report

Once you've completed your assessments, testing, and audits, you need to generate a report that helps you, the team, and management understand the findings of these activities. If you're performing the assessment and audit as a separate project in preparation for the development of your corporate IT security plan, these findings will form the basis of that project plan's requirements and assumptions. If you're performing these tasks as the first major objective within your corporate IT security project plan, you'll need to take these findings and circle back into some of your earlier planning tasks to revise your plan based on the results of this first phase. In either case, it's not enough to simply record the results of various assessments, including vulnerability assessment and auditing. This data needs to be turned into actionable information that is incorporated into later stages of your project. Information without action is as bad as no information. You and your team should spend time thinking about the types of data that will result from these activities and how that information can be used to increase security across the enterprise.

The results of your assessments and audits might become legal documents if your network is later breached, so you should be cognizant of the potential implications of these reports. That is not to say you should omit or minimize negative information. To the contrary, you should document the issues found with the clear understanding that you will take action—within a reasonable time and in a reasonable manner—to mitigate or resolve these issues.

It is easy to forget that this document essentially lays out every vulnerability and weakness discovered. What a great resource for a hacker! Be sure that the document is not widely distributed and that you maintain strict control of it. You may choose to create several versions of this document, most of which do not specifically delineate the vulnerabilities and weaknesses in a way that could be exploited (e.g., your executive team does not need to know the all the details, and you don't need to worry about where the document ends up. There might also be some legal liability issues with regard to executives being made aware of specific problems.

You may want to sit down with your project sponsor to discuss the reporting requirements for this project. Since there are potential legal issues related to this type of reporting, you may also want to consult with your firm's legal counsel before you begin your security project plan, to determine the most appropriate way to proceed. Again, the intent is to ensure that your firm stays within the realm of legal and ethical behavior; your job is to help your company navigate that sometimes circuitous path.

Elements of a Findings Report

The elements that should be included in your report should be, at a minimum:

- The steps taken to assess vulnerabilities and weaknesses
- A list of vulnerabilities and weaknesses found
- An assessment of the risk (criticality and likelihood of occurrence) of each vulnerability or weakness
- The specific steps to mitigate each vulnerability or weakness
- The specific owners, timelines, and deliverables for each mitigation strategy

Let's look at these elements in more detail.

Defining the Steps Taken

Through the Work Breakdown Structure (WBS), your project plan should describe all of the steps taken to assess, test, and audit security across the enterprise, so that you can easily recap these activities in the beginning of your report. Rather than put copious amounts of detail in this section, you may choose to put a reference or link to the project plan itself.

Defining the Vulnerability or Weakness

After the assessment, you should have an excellent idea of what vulnerabilities were found. You should describe in detail the source and nature of each vulnerability. If possible, organize them using some logical system, whether by system (external, network configuration, servers and hosts, and so forth), or by source (network protocol, operating system, scripts, and so forth). Beware of standard security definitions that come "out of the box" with various security applications. They are intended to be one-size-fits-all definitions, but they often don't fit. Use the expertise of a security professional (whether internal or external) to define the importance of the vulnerabilities.

Defining the Criticality of Findings

Each vulnerability or weakness should be assessed for criticality (i.e., how important is this vulnerability?). As you know, there are some vulnerabilities that would be devastating if exploited, but the likelihood of such an exploitation is statistically insignificant. Remember that your findings report may serve two purposes: internal and external. The internal purpose might be to document findings in preparation for an IT security project, or it might be used as a tool to negotiate for a higher IT security budget based on vulnerabilities discovered. On the external side, this may become a legal document if something goes wrong down the road. Be aware of the potential uses of this document. Create a document with the right amount and level of detail regarding your assessment of the criticality and potential impact of vulnerabilities.

You can use whatever ranking system works for you. Some people use a numbering system where 10 is the highest criticality and 1 is the lowest. Others use words such as critical, high, medium, and low. Whatever ranking system you use should be defined so that everyone understands the meaning. What does "critical" or "10" mean? You could say that "critical" is defined as any activity that can cause bodily harm or death, significantly compromise the company's financial future, significantly compromise the company's ability to remain an ongoing concern, significantly damage the company's brand or reputation, or result in significant legal liability or lawsuits.

Defining Mitigation Plans

Your mitigation plans might be part of this project plan or they may feed into your larger corporate IT security project plan, because a solid assessment should be the starting point for most (if not all) IT security projects. Therefore, how you address your mitigation plans will depend on how you're approaching the project as a whole.

Mitigation plans should be clear, specific, and measurable. They should include which specific vulnerability they are addressing, how the vulnerability will be mitigated, and what the result should be. It might also include how you'll test the results of the mitigating action as well as how these results should be rolled into ongoing security processes and procedures. Finally, it should include recommendations for changes to physical, technical, and administrative policies, as appropriate.

Defining Owners, Timelines, and Deliverables

In the project management world, a task with no owner most likely will not get done, or the task will default to the project manager. To avoid either of these scenarios, you should include owners, timelines, and deliverables in your finding report. If these tasks are going to be rolled into a higher level corporate IT security project plan, you should still define these elements and then make sure they are incorporated into the details of the corporate plan. Deliverables might include functional, technical, legal, financial, or regulatory requirements. They might also include specific acceptance criteria and should include success criteria. If you recall, acceptance criteria are those standards by which a project result is accepted (typically by a client, but in this case it might be acceptance by a regulatory or compliance authority). Success criteria are those standards by which the task owner knows the task was successfully completed. They are closely related, but are not the same in every case.

Format of a Findings Report

You don't necessarily need to hire a graphic designer to format your findings report for you, but you should create a professional presentation. If you're going to present it to senior management, it should be well-prepared so that it provides information in a clear, concise, and professional manner. It should be technically accurate and as objective as possible. While it's tempting to become a bit defensive if the results are not stellar, it's more important to stick to the facts. Executives typically hate spin and obfuscation, therefore, your best bet is to calmly and rationally state the facts. That also means that you should avoid presenting the information in an overly pessimistic way as well. Executives also don't like to hear "the sky is falling," even if it is. Try to be fair and balanced. One way to do this is to include measurable statements. This helps prevent an "all or nothing" presentation.

The actual presentation for your findings will vary based on your corporate culture. If creating a PowerPoint presentation is how you disseminate information, go for it. Otherwise, write the report in a format that's aligned with the relative formality of your organizational reporting norms. For starters, here's an outline you can use to begin the process:

1. **Cover Sheet** Cover sheet with title, author name, contact information, and date.
2. **Table of Contents** If the document is long, a TOC is helpful.
3. **Executive Summary** Write this after you've completed writing the report. Think of what you'd say if you ran into an executive in the elevator and had one minute to summarize your findings.
4. **Summary of Findings** Discuss the project background briefly as well as the scope, key findings, and methodologies used.
5. **Detailed Findings** Include relevant detail that you want to capture and report. You may choose to leave some detail out and reference an external document that contains all the detail, depending on how much detail is available. A 9,000 page detail document might not be helpful for anyone but the IT staff.

6. **Remediation** If you haven't included remediation recommendations or actions in your findings, include them here.
7. **Timelines and Deliverables** Any follow up action required should have assigned owners of specific tasks. These tasks should define clear timelines and deliverables.

We'll discuss more about various security reporting processes and tools when we discuss operational security later in this book. For now, we're focusing on reporting needs during the assessment and auditing phase.

Project Plan

We've covered a number of related topics in this ISAP, including managing assessments, audits, access control, authentication, attacks, and reporting. Now you should have the data needed to put together your security project plan. As with all projects, let's start with the problem statement and the major objectives. Once those are defined, you and your team will be in a better position to select the optimal solution for your organization.

Project Problem Statement

Your problem statement for this security project plan should focus on the need to ascertain how secure your network currently is, what processes, procedures and systems are in place to maintain security, and how that security can be supported, maintained, or enhanced. The problem statement you generate will be specific to your organization. However, three statements are provided here as generic starting points.

> We do not have a benchmark for our current level of security, and we are not confident that our network is as secure as it can be given our size, resources, and vulnerability profile.
>
> As our company has grown, our public profile has also grown, and we are concerned that our network may now be

> a valuable and sought-out target for attacks. We are particularly concerned about maintaining confidentiality of certain data.
>
> Our company is now subject to several governmental regulations regarding the confidentiality, integrity, and availability of our data. We are not confident that we currently meet those standards; we need to ensure that we meet or exceed them within the next six months.

Problem Mission Statement

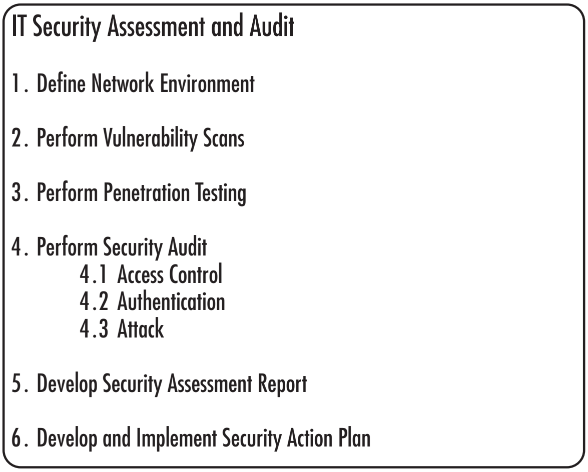
As with the problem statement, your mission statement will be highly unique to your company and this project. However, here's a starter for you:

> To assess how well IT security systems protect the confidentiality, integrity, and availability of critical network resources, and to generate specific actionable data that can be used to increase security across the enterprise.

Project Objectives

Once you've defined your problem and mission statements, you are ready to create a short list of high-level objectives. In this project, we're focusing on assessing and auditing your network for vulnerabilities. You can lay out your objectives in one of several ways, depending on your preferred approach to IT project management. Some people like to combine their major objective and follow-up action into one objective (i.e., if you test for vulnerabilities, you also want to create a process for addressing those vulnerabilities, which can all be put into one high-level objective. On the other hand, you could make vulnerability scanning one high-level objective and remediation another. Thus, the objectives for this individual security area project look something like the list shown in Figure 10.4.

Figure 10.4 Sample Objectives for Security Assessment and Audit Project



IT Security Assessment and Audit

1. Define Network Environment

2. Perform Vulnerability Scans

3. Perform Penetration Testing

4. Perform Security Audit
    - 4.1 Access Control
    - 4.2 Authentication
    - 4.3 Attack

5. Develop Security Assessment Report

6. Develop and Implement Security Action Plan

We've talked about each of these elements throughout this chapter. The objectives here are clear and will form the foundation of the project's WBS. Your security project plan's objectives may vary from those shown in Figure 10.4, but the overall result should be the same—a list of high-level objectives you want to accomplish in this project.

Potential Solutions

Your potential solutions are varied, but let's start with the fact that you can perform these assessments and audits internally using IT staff, or you can outsource this function. There are pro's and con's to both approaches and you may have a third or fourth viable option you want to consider. When you look at your potential solutions for this particular ISAP, you need to consider the following factors:

- Do we have the internal expertise we need to ensure we're effectively looking at all systems?
- Do we have the time to perform as extensive an assessment, audit, and test as is needed?
- Do we have the budget or time to train internal staff to perform these tasks? If so, is that desirable?

- Do we have the budget or time to locate and retain an external firm to perform these tasks? If so, is that desirable?
- Do we have the tools and resources we need internally to perform these project tasks? If not, is the cost of acquiring and learning them a wise investment?
- Is there any benefit to not acquiring the needed tools internally?
- Are we confident we have trustworthy individuals internally that will perform these tasks as needed?
- Are we confident we can hire an external firm that we trust to perform these tasks as needed?
- Are there organizational or political considerations that will impact this decision?
- Are we subject to specific legal or regulatory requirements that would impact this decision? If so, what are they and how will they impact this decision?
- Are there other organizational resources we can call upon to assist with some of the non-technical elements of this project?
- What are the environmental constraints (technology changes, industry changes, pending litigation, pending acquisition, and so forth) that might impact this project?

How you approach your list of potential solutions is up to you, but if you ask and answer these questions, you'll at least start out with a clear idea of some of the factors impacting your decision. These questions (and any others you want to add to the list) should be addressed by the core IT project team with key stakeholders, if possible. Remember, user input early in the process will help avoid disconnects that often lead to security problems later. While users may not understand some of the more technical elements of the project (e.g., vulnerability testing or assessing the risk of various types of attacks), they can be very helpful in letting you know how current security is working and how they work with the current security processes. In fact, they may very well have great ideas on how security could easily be improved that you might never think of.

Selected Solution

Once you've looked at your potential solutions and thought through all of your organizational constraints and considerations, you should be able to identify the optimal solution for this project. Remember, at this point you want to focus on the optimal solution, knowing that you'll more than likely have to scale it back in one way or another once you start addressing project constraints. In some ways, organizational constraints are project constraints, but it's often helpful to separate them into two distinct categories.

Organizational constraints that impact your solution selection might include the fact that the president of your company sits on the board of a company that uses solution X, and has therefore mandated that you consider using solution X. It might be that you know your company is in the process of acquiring another company and that your IT budget will be strained with acquisition-related activities. These are organizational constraints you'll have to deal with. Once you begin defining your project, there will be additional constraints (e.g., a specific project budget, allocation of resources, and project timing that will impact the project even more directly). You'll have to bounce your ideas about your optimal solution against these organizational constraints to see what is most optimal at this juncture. The key is to start from the best possible solution and shave it back from there. If you start placing too many constraints on your project at the solution selection point, you may miss an opportunity to create an optimized plan. It's like digging around in your pocket to see how much cash you have and then deciding what to have for lunch. You may have failed to take into account that you also have your debit and credit cards with you, which would open up more possibilities. Don't limit yourself too early in the process.

When you have identified your optimal solution, take time to clearly describe and record it. The last thing you want is to sit through long meetings to reach consensus only to have to re-visit the decision in 30 days when a new vice president comes on board. While you might still have to re-visit the decision, if you have adequately documented the process of coming to the solution, the rationale behind it, and the factors considered, you may be able to short-circuit these kinds of endless loops that can drive even the most sane IT person over the edge.

General IT Security Project Parameters

We've defined our project's problem, mission, and objectives very clearly. Next, we need to define the project's environment. Again, the specifics of these sections will vary from company to company and from project to project, so don't just cut and paste these into your plan. That said, you can use these if they apply directly to your unique set of circumstances. You'll need to look at the requirements for this particular project as well as define the scope, schedule, budget, and quality of the project. Once you understand what's involved (at least in a preliminary way), you also need to describe the skills you'll need to successfully carry out the project. After the required skills are documented, you'll need to assign key personnel to the project and form your project team. The final stage of the definition stage is to develop and document project processes and procedures. Ideally, you're already working with a core project team, but if not, this is a good time to pull in additional resources to help in the initial project definition stages.

Requirements

What are the requirements for a project whose objectives include performing security assessments and audits as well as developing recommendations for remediating or removing any vulnerabilities discovered? As discussed in earlier chapters, there are a wide range of requirements that often impact IT projects. We're not going to run through all of them again, but we will provide a quick list of the major categories of requirements you should consider including. Then, we provide a few specific requirements for this type of security project plan and let you take it from there.

Types of Requirements

The following are the types of requirements you should consider including in this project. Also, check with your team, your human resources group, your legal representative and your project sponsor before finalizing your requirements list.

- User requirements
- Functional requirements
- Technical requirements
- Legal or financial requirements

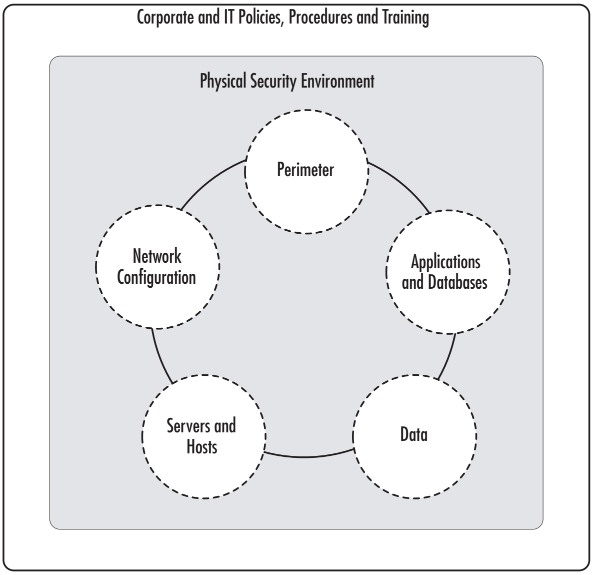
Project Specific Requirements

The types of requirements needed for an assessment and auditing project plan include the technical requirements for the various assessments and tests to be performed. When looking for security vulnerabilities, you should specify the specific target of the assessment, the specific tests or actions that will be taken, how results will be monitored, recorded, and reported, and how recommendations will be made. These might fall under functional, technical, legal, or financial requirements. Technical specifications should encompass methods, tools, and techniques that will be used to test and assess security. The audit function should include very clear specifications regarding functional and technical requirements.

While you might not specifically think of user requirements in this type of project, a user requirement in this context might include that tests be run at night or on the weekend when the fewest users will be impacted; that users be selected at random (or via some specified system) to review current security practices; or that users will be needed to perform certain testing or auditing functions due to specific subject matter expertise that you want to bring onto your IT project team.

You may choose to develop your requirements using the elements shown in Figure 10.5 as your guide. Look at your perimeter, network configuration, servers and hosts, applications and databases, and data needs as you develop this project's functional and technical requirements.

Figure 10.5 Element of IT Security Requirements


Corporate and IT Policies, Procedures and Training
Physical Security Environment
Perimeter
Applications and Databases
Data
Servers and Hosts
Network Configuration

Scope

The scope of this project is up to you and your team. If you choose, you can parse out these different topic areas (as shown in Figure 10.5) into separate sub-project plans that roll up into your general IT security project plan. If so, each of the sub-project's scope would be limited to the topic area. If we assume these elements are part of one project, the scope is all the work to be done to assess, test, and audit security in each of these areas as well as the security at the intersection of these areas.

The scope statement should be as specific as possible about what the project includes and what it doesn't include. Here are a few examples of statements that help you define the scope of your project:

1. The company has 47 servers, including infrastructure, systems, and applications servers, which are all included in this project. The organization may acquire the business operations of CompanyZ during this project and CompanyZ servers are specifically excluded from the scope of this project. CompanyZ servers will

be included in a separate project plan should the acquisition go through.

2. The company has 3,243 host computers, including 2,844 desktop computers and 399 laptops and other mobile devices. These are all included in the scope of this project. All CompanyZ host computers are excluded from this project.
3. The company has four separate geographic locations. Each location is a separate domain within the corporate forest. Each of these four domains is included in this project plan. Domains external to these four domains are specifically excluded. The four domains are: *east.company*, *west.company*, *north.company*, and *south.company*.

Each of the above statements is a clear, specific statement. We could continue to delineate which operating systems the servers and hosts are using, and we could specifically exclude all operating systems that are not listed as currently under use. Or, we could have delineated all the operating systems and specifically included or excluded Linux and Apple operating systems in this project.

The key is to be very clear about what you're going to include in this project. Later, as you develop your WBS, you can keep an eye on your scope statements to make sure you don't define a larger project than your scope statements describe. On the other end of your WBS development, you can circle back and determine if your WBS describes a bigger project than your scope statements. A good checks-and-balances approach to developing and defining your project helps mitigate scope creep.

Business Intelligence…

Scope—Best Practices

Scope creep happens in even the best-planned and managed projects. The key is how well you can manage that creep so it doesn't get completely out of hand. While it's true that there are some projects in which scope does not creep, it seems to be one of the most common areas to shift and change as a project moves forward. One way to contain or even prevent scope creep is to define not only what the project includes, but also what it specifically excludes. The project management gurus in Stanford University's Advanced Project Management program suggest defining what a project is and is not. Sometimes by forcing yourself to specifically say what is not included, you can better define the boundaries of scope and prevent it from oozing out in all directions. It may not cure all scope creep problems, but it will help you draw a line in the sand.

Schedule

You're most likely familiar with the concept of the WBS, which is your detailed list of project tasks broken down into manageable work units. Until you develop your WBS, you can't create a detailed or meaningful schedule. However, at this juncture, you should have a sense of how much work this assessment, testing, and auditing project is going to require. Therefore, you should at least begin to develop your first pass schedule. Will this take 6 weeks or 6 months or 60 months? Based on the high-level objectives and your scope statement, you should begin narrowing this down to a ballpark duration for the project, with high-level milestones you might want to include. For example, you might look at your objectives and scope and determine that this is about a 4-month project. You might also know that your company is being investigated by the SEC for potential violations related to the disclosure of confidential data and that your project will come under intense scrutiny. Therefore, you may choose to shorten this proposed schedule, knowing it will cost more to get it done quicker, so that you can complete your assessment within 60 days in order to comply with one of the SEC's recommendations (or requirements). Remember, too, that if you shorten your estimated project time, you'll have to modify the scope, budget, or quality to compensate.

Budget

As with your schedule, you're not completely ready to sign on the bottom line for the project cost estimate, but you should have a sense of what this project will likely cost. If your company has a set budget for this project, you have to find ways to work within that pre-determined budget by adjusting the scope, schedule, or quality. On the other hand, if there is no set budget for this project at this time, you can develop a high-level guess based on your experience and expertise. If possible, avoid tossing around schedule or budget estimates at this point, as they often "stick" and you end up with a ballpark estimate becoming your actual schedule or budget.

Once you develop your detailed WBS, you can better estimate the time and cost of each task and activity and roll it up into a project budget. Remember to involve subject matter experts who can best estimate both time and cost for specific tasks within the project plan.

Quality

Defining quality in the assessment, testing, and auditing area is tricky. If you determine that zero intrusions is your requirement, then your quality metrics are very high. You will always have to balance security against cost and against usability. Where you draw these lines is how you are, by default, defining quality. If you tolerate some security vulnerabilities or weaknesses due to user requirements or cost constraints, you have essentially lowered the quality. This is not necessarily a bad thing as long as it's done consciously and intentionally, and as long as you can justify the reduction in quality. As stated, you don't need the same security as the U.S. Treasury if you're selling granite to landscape companies. Keep this in mind as you define what level of quality is acceptable.

By the same token, be cognizant of the costs of reduced quality in terms of potential legal liability. This may be an area in which you choose to consult with your legal representative to determine what "reasonable care" in your company and industry would consist of. While there may be no definitive answer, getting expert guidance can reduce your overall risks, especially when it comes to making decisions about the trade-offs between security and cost or security and usability. Although quality is a difficult area to tackle, quality goals and metrics help define the maturity of the processes that are in place. The ultimate goal is continuous improvement, but you have to start on a very solid foundation to build quality into all of your security and IT processes.

Key Skills Needed

In a project of this nature, you need a variety of skill sets. First, you need extremely savvy technical people who can think and test like hackers. This is a slippery slope, indeed, because it's always a bit unnerving to have people on your IT staff who think like hackers. On the other hand, is it any safer or more reassuring to hire an external firm that thinks like hackers and hand them the keys to your system? As the old expression states, "better the devil you know than the devil you don't." There is no single right answer, but you should be aware of the risks. You'll also need people who are less technical, who would be excellent at reviewing policies and procedures as they relate to security practices in the company. These people are sometimes found in the IT department, but might also be found elsewhere in the company. This list is not exhaustive but should give you an excellent running start.

Technical Skills

1. Physical layer protocols, processes, and services
2. Network layer protocols, processes, and services
3. Operating systems
4. Applications

5. Databases
6. Internet
7. Wireless
8. Intrusion Prevention System (IPS) and IDS
9. Attack methodologies
10. Attack testing tools
11. Vulnerability and intrusion testing tools
12. Reporting tools
13. Remediation tools, techniques, and recommendations

Non-Technical Skills

1. Public information reconnaissance (what information can be found about your company)
2. Review of security policies
3. Review of procedures and policies (might also require technical review or assistance)
4. Recommendations for implementation (from a non-technical and user perspective)
5. Documentation
6. Training
7. Project communication

Key Personnel Needed

Once you've defined your technical and non-technical skill sets, you need to locate and acquire the right people for the project. In any project, this can be a challenge for a number of reasons. However in the case of a security assessment, you need to be sure you have the right players on your team. If you don't have the depth and breadth of skills needed, you will have to devise a strategy for acquiring those skills. Depending on a number of variables, you will have to decide whether to train, hire, or contract out for those skills. Whatever route you take, be sure you have people who are well-versed and experienced in the technologies related to security vulnerability and testing, as well as assessments and audits. This is one area where you could have some serious gaps in skills; it's better to address them now than face a potentially devastating security breach later. Since you can't personally perform and monitor every single task in this project, you need to have a high level of confidence that the team you do have has the requisite skills, because at the end of this security project plan, you will be held accountable for results.

Form the Project Team

Forming the project team is listed here to remind you that if you haven't yet put together a preliminary team, you've missed a few opportunities to actually gain expert input and assistance. However, if you've been working with your core team up until this point, now is a good time to begin defining the ongoing project team, which might mean creating several sub-teams to address various sub-sections of the project based on expertise, availability, or other pertinent factors. At this point, you should have a clear idea of how readily available your needed resources are and what strategies you'll need to use to acquire the right talent at the right time in your project lifecycle.

Project Processes and Procedures

With your project team, you should define the processes and procedures for this project. You should have many standard templates for things like task status reporting (to you), project status reporting (to management), project status reporting (to the user community), issue tracking, escalation procedures, and more.

In addition, you need to define very specific procedures and processes for implementing your assessment, testing, and auditing (e.g., if you hire outside contractors to perform these tasks, you should have very clear legal documents drawn up that might include non-disclosure agreements, specific agreements about what to test and when to test it, and specific guidelines on what should be done with the resulting information.

Even if you're working internally, pen testing is a tricky situation, because you don't want employees getting in trouble for performing a pen test and exposing a serious vulnerability. Be sure you get the proper authorization and document the specific people, responsibilities, tasks, and timelines. These should be part of your project processes and procedures in this type of project, due to the sensitive nature of this kind of work. Remember that pen testing on the front side is most useful to test areas that you believe you've previously secured, not to just go after the network prior to implementing your security plans.

You'll also need to define what should occur in the event a vulnerability scan or pen test reveals a very serious problem. If you've defined "very serious" as "critical" or as a "10," what should the tester do? These should be thought of in advance to protect everyone involved. Deciding on these actions ahead of time helps set expectations and helps keep everyone calm when something significant occurs.

General IT Security Project Plan

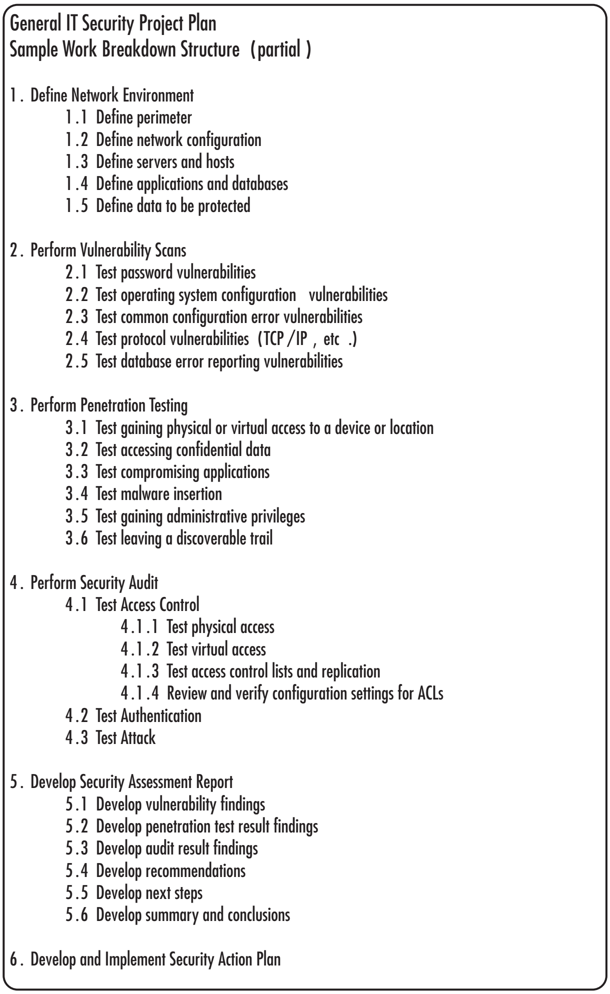
We've defined the environment for the project, now it's time to get into the details of the project plan. The next step is to take the high-level project objectives and create the WBS. Whatever method you use for creating the WBS is fine, but remember to follow a few best practices:

- Use the verb/noun format to describe tasks so they are clear and unambiguous.
- Don't spent time placing tasks in order until later; just make sure they all get captured.
- Gather subject matter experts to assist in developing a detailed WBS.
- Use a numbering scheme that helps you understand the relationship between and among tasks.

Project WBS

Your WBS will vary depending on the specific objectives you've developed for this project plan. However, to give you a running start, we've included a sample in Figure 10.6. If you're familiar with developing a WBS (which we're assuming you are), you can follow whatever methodology you're most comfortable with. If this is all new to you, you can use the structure shown in Figure 10.6 as a solid starting point. Be sure to include reporting and close out activities in your project plan, as you would with any type of IT project.

Figure 10.6 Sample WBS for General IT Security Project Plan



General IT Security Project Plan
Sample Work Breakdown Structure (partial)

1. Define Network Environment
    - 1.1 Define perimeter
    - 1.2 Define network configuration
    - 1.3 Define servers and hosts
    - 1.4 Define applications and databases
    - 1.5 Define data to be protected

2. Perform Vulnerability Scans
    - 2.1 Test password vulnerabilities
    - 2.2 Test operating system configuration vulnerabilities
    - 2.3 Test common configuration error vulnerabilities
    - 2.4 Test protocol vulnerabilities (TCP/IP, etc.)
    - 2.5 Test database error reporting vulnerabilities

3. Perform Penetration Testing
    - 3.1 Test gaining physical or virtual access to a device or location
    - 3.2 Test accessing confidential data
    - 3.3 Test compromising applications
    - 3.4 Test malware insertion
    - 3.5 Test gaining administrative privileges
    - 3.6 Test leaving a discoverable trail

4. Perform Security Audit
    - 4.1 Test Access Control
        - 4.1.1 Test physical access
        - 4.1.2 Test virtual access
        - 4.1.3 Test access control lists and replication
        - 4.1.4 Review and verify configuration settings for ACLs
    - 4.2 Test Authentication
    - 4.3 Test Attack

5. Develop Security Assessment Report
    - 5.1 Develop vulnerability findings
    - 5.2 Develop penetration test result findings
    - 5.3 Develop audit result findings
    - 5.4 Develop recommendations
    - 5.5 Develop next steps
    - 5.6 Develop summary and conclusions

6. Develop and Implement Security Action Plan

Project Risks

There are always risks to any project and this one in particular is fraught with possibilities. You and your team should spend time discussing your project's risks as well as your plans for mitigating those risks. Included should be your triggers (how will you know the risk has occurred) as well as your assessment of the potential risks involved in your mitigation plan.

Risks to this type of project include (but are not limited to):

- Missing a significant vulnerability or weakness
- Failing to fully implement recommended solutions
- Changes to corporate objectives, structure or funding

You can define as many risks as you choose. As with other risk assessments, you should determine the likelihood of the risk occurring and the impact should it occur. Then create mitigation plans for those risks that weigh in on the top of your list. The biggest single risk is that your project will fail to find a significant vulnerability or weakness. The bigger risk is that you will fail to find it and someone will exploit it. How do you mitigate this type of risk? In part, through sound project planning and consistent methodologies. Don't let egos drive this process. If you believe your team members have the requisite skills, fine. Otherwise, find outside resources to assist you.

Project Constraints

Constraints on any project often include time and money, but more specific to this project plan, one of the typical constraints, is the ability to perform these assessments. Non-intrusive attacks are generally safe and can often be performed at just about any time. On the other hand, intrusive attacks are more dangerous and could potentially disable a server, network segment, or the entire network. Therefore, the timing of these various tests is often constrained by user schedules and higher level corporate events. It would be pretty dismal if your testing brought down the network on the same day your boss was holding a press conference in the conference room using network-based resources.

Another common constraint in this type of project is the availability of highly qualified personnel. This project requires a very specific set of skills for many aspects of the assessment and testing functions. Having the wrong people performing this work can result in wasted time or increased vulnerabilities. However, you may have difficulty finding, training, hiring, or contracting out for these services, especially if your budget is locked in. This is the place in your project plan where you review and work through these various constraints to determine what impact they will have on your project. If they are significant, it will require you to sit down with your project sponsor to work through these problems before proceeding. If you believe the constraints on this project are serious, don't agree to a project plan that is faulty from the start. Negotiate with your project sponsor to address these problems.

Project Assumptions

Project assumptions in this type of project might include a list of the known vulnerabilities you'll be testing for, and the assumptions about the skills or availability of key technical resources. If you have two people on your team who are able to perform the bulk of the vulnerability scanning and testing, you should list this as an assumption about your project.

While some project management methodologies list "success factors" as discrete elements of the security project plan, they can also be incorporated into assumptions. If you assume that the things you need to be successful are included, you can list them in this section (e.g., if continued executive support is one of the factors you deem essential to the success of the project, or if you believe that a 25 percent increase in your IT budget will come through and is fundamental to the success of the project, list these as assumptions.

Project Schedule and Budget

Now that you've developed your WBS, you have a list of the tasks needed to successfully complete this project. Therefore, you should be able to look at your tasks and develop a more detailed schedule and budget. The schedule must take into consideration the various constraints as well as resource scheduling, corporate event coordination (e.g., avoiding an outage during a press conference or VIP tour of the facilities) and task dependencies.

Projects with more milestones tend to be more successful than those with fewer milestones. Add milestones as checkpoints throughout your project, so that you can keep the team focused on the next steps and you can measure progress more effectively.

Once you've concluded these tasks, you're ready to launch, manage, and close out the project.

Summary

In this chapter, we looked in detail at how to develop a security project plan for a security assessment and audit project. It should form the foundation of any IT security planning process, whether you undertake the project as a standalone project or as part of a larger corporate IT security project plan. We looked at different ways to view the security assessment as a whole, including looking at the perimeter systems, internal network, server and host systems, applications and databases, and data. It's important to understand the elements that comprise an assessment, which typically fall into the vulnerability scanning, pen testing, and risk assessment with the caveat that any pen testing should be limited in scope prior to implementing a security project. The audit function includes auditing physical, technological, and administrative policies and procedures. We also looked briefly at access control, authentication, and auditing as part of our overall security assessment, and will re-visit some of these topics briefly in our operational security project plan. Finally, we developed a security project plan that includes a problem statement and a mission statement, potential solutions, the selected solution, and the high-level objectives. We also developed other project details including the skills required, the WBS, the project risks, and the assumptions.

At this point, you should have a solid start on your general IT security project plan focused on assessment, testing, and auditing. While this initial project plan will not be your end-point, it should give you a reasonable start on defining and planning a security project plan customized to your company's unique situation.

Solutions Fast Track

IT Security Assessment and Audit

☑ A security assessment and audit is a typical starting place for any IT security project.

☑ People, processes, and technology must all interact effectively to maintain and enhance security.

☑ It's often helpful to categorize the components that should be included in your assessment. One way to parse these out is: policies, procedures and training; physical security; perimeter; network configuration; servers and hosts; applications and database; and data.

☑ The types of assessments usually include vulnerability scanning, pen testing, and risk assessment.

☑ Pen testing prior to implementing a security plan should be limited and very focused. Gaining access through an open door doesn't prove the locks don't work.

☑ Types of auditing include authentication, access control, and auditing (at a systems level).

☑ An impact analysis helps define what would happen if these vulnerabilities or weaknesses occurred. This can help you prioritize activities and expenditures.

Authentication

☑ Authentication proves the identity of an entity trying to gain access to network resources.

☑ There are many different kinds of authentication schemes available today. They span many different network types, operating systems, and devices.

☑ Authentication is managed through a variety of methods and each should be assessed and tested during this project.

Access Control

☑ Access control limits access to devices, resources, and data in the organization, based on pre-existing rules and policies.

☑ Access control can be developed on several levels, including physical, local, and remote.

☑ Testing access control spans all systems and networks, and requires a thorough audit of processes, procedures, and configuration data.

Auditing

☑ Auditing is used in two ways with regard to this project. There is the task of auditing current security settings and there is the ongoing activity of auditing key network activities.

☑ Auditing current security settings includes reviewing physical, technical, and administrative policies.

☑ Auditing should also include a thorough review of processes and procedures, operational issues, and any legal and reporting issues.

Attacks

☑ Your vulnerability scan and pen testing should include various known attack types.

☑ Your plans should also include an assessment of your firm's attack footprint and plans for reducing that footprint.

☑ Attacks can be non-intrusive or intrusive. Non-intrusive attacks typically involve gathering information in preparation for an intrusive attack.

☑ Intrusive attacks typically include stealing, modifying, or destroying critical data or systems.

☑ A list of attacks as well as the likelihood of or vulnerability to various attacks should be included in the security project plan, to ensure a comprehensive plan and to document what should be included.

Assessment and Audit Report

☑ Once you've completed your assessment, testing, and auditing activities, you will need to generate a findings report.

☑ Remember that the data contained in this report enumerates your company's vulnerabilities, and may become a legal document. Handle this document with extreme care and maintain close control over it.

☑ Include the following items in your report:

- Define what steps were taken
- Report the results of the steps taken (vulnerabilities and weaknesses found)
- Define the criticality of findings
- Describe mitigation plans
- Define owners, timelines, and deliverables.

General IT Security Project Parameters

☑ As with any project, your planning process should begin with clearly defining the problem statement, mission statement, and high-level objectives

☑ After defining the basic elements, you and your team should look at all potential solutions and then select the optimal solution. If you don't look at all potential solutions, you might inadvertently overlook an excellent but somewhat unconventional solution.

☑ An assessment and auditing project has a very specific set of requirements. Carefully define functional and technical requirements to ensure you create a thorough assessment plan.

☑ The scope of your assessment and audit plan may be part of a larger corporate IT project plan, or it may be a standalone project. Clearly define the scope by describing what is and is not included.

☑ You won't have enough detail at this juncture to commit to scope, schedule, budget, or quality, but you should begin defining these so they can be refined as you gather additional information.

☑ Don't let egos drive your decisions about needed skills and personnel. Your company's future may rest on the skills and expertise of the people you select, therefore, be diplomatic but honest in your assessment.

General IT Security Project Plan

☑ Your WBS should be developed from your high-level objectives specific to assessment, testing, and auditing activities.

☑ Include reporting and close out activities in your WBS.

☑ Risks in security assessment and auditing type projects require that specific attention is paid to the risks of not finding vulnerabilities and weaknesses, and the risks of finding those weaknesses and not addressing them adequately.

☑ Assumptions should be examined and well-documented, because the success of the project ultimately rests on the assumptions you make about the project and its environment.

☑ Assumptions can also include critical success factors. If a budget of $100,000 has been discussed and you believe it is critical to the success of the project, state that as an assumption.

☑ Once you've developed a detailed WBS, you can hone your schedule and budget.

☑ Be sure to include reporting and close out activities, and roll these into your corporate IT security project plan, if appropriate.