Chapter 13

IT Operational Security Plan

Solutions in this chapter:

- Operational Security Assessment
- Project Parameters
- Project Team
- Project Organization
- Project Work Breakdown Structure
- Project Risks and Mitigation Strategies
- Project Constraints and Assumptions
- Project Schedule and Budget
- Operational Security Project Outline

☑ Summary

☑ Solutions Fast Track

Introduction

Network security is no longer just a technical issue, it's a business issue. It's no longer just a problem for the IT department to handle, it's an organizational problem. In the past, IT security was viewed as an expense, but slowly, companies are beginning to see it as an investment. It has evolved from an ad hoc activity to one that is planned using proven methodologies. Perhaps the most important shift occurring is that organizations are beginning to move from the reactive "security incident response" mentality to the "organizational resiliency" (thanks to folks at CERT/CC for that phrase). Companies are facing the stark reality that security is no longer just something a few geeky guys do in the dark recesses of the IT department. Corporate executives understand that while network services have moved more toward "utility" services, security has moved toward a more specialized commodity that involves the entire organization.

Operational security is sometimes overlooked or put together in a patchwork fashion. That's unfortunate because all the hard work that went into your IT security projects is pretty much wasted if you don't develop on-going operations that support or enhance security. This is accomplished through your operational security plan. In this chapter, we're going to look at five distinct areas that support security: incident response, corporate and IT policies related to security; disaster recovery (whether a hurricane or a network intrusion), regulatory issues, and configuration management. These are not the most exciting topics to techies, which is probably why they're often neglected. If this topic bores you to tears, find someone on your team who loves policies and procedures and get him or her fired up about this project then hand it over. Whatever you do, don't squander a great opportunity to tighten up security on the front and back end of your technology initiatives.

Operational Security Assessment

As with all security initiatives, it's wise to begin with an assessment of your operational security. We'll continue to use the five topic areas mentioned in the Introduction to guide us through our assessment and our planning activities:

- Incident response
- Security policies
- Disaster recovery
- Regulatory compliance
- Configuration management

The first operational area is obvious – what do you do if there is a security incident? If you don't have a planned response, you're likely to overlook something (or create a bigger problem) in the aftermath of an attack. You and your team may be scrambling to lock the doors and forget that the window is wide open. How you respond to incidents can mean the difference between being down for an hour or a month.

Policies are a part of every organization, whether they're formal or informal, written or practiced. It's important to define policies that support security without creating a convoluted tangle of rules and regulations that only serve to confuse users. Confused users are dangerous users because rather than try to understand what they should and should not do, they'll do whatever they know how to do or whatever is easiest. This type of user behavior neither supports nor enhances security.

We often think of disaster recovery in the context of natural disasters such as fires, floods, earthquakes or hurricanes. However, unnatural disasters include network intrusion, data modification, data falsification or data corruption. In these cases, it's important to have a clear path to recovery. If you recall from Chapter 1, companies that fail to restore lost data within 24 hours of an attack or system failure have a 50 percent chance of going out of business within three years. Those are seriously bad odds, and they don't bode well for IT job security either. Having a viable disaster recovery plan in place may not only save your job but it may well save your company.

Throughout this book, we've discussed regulatory issues that impact your IT security projects. While it's outside the scope of this book to cover all of them in detail, we will take a more in-depth look at some of the issues facing companies in the compliance and regulatory arena so you can determine next steps for your own organization.

Configuration management, though individually called out, is really incorporated into a number of different areas. Configuration management is an important part of maintaining a secure and compliant network environment. It should be incorporated into your response team's security management and proactive services definitions; it should be done through developing policies and procedures for your IT staff's day-to-day operations, and it should be done on a consistent basis and incorporated into disaster recovery plans on a regular basis. Configuration management is a large topic and might be a large enough issue in your organization to warrant its own distinct project plan. You can find additional information on configuration management online. A good place to start is: http://en.wikipedia.org/wiki/Configuration_management#Sites_for_configuration_management.

Business Intelligence…

Risk Assessment Tools

There are many great tools available for performing risk assessments. Here are four you might want to investigate.

Operationally Critical Threat, Analysis, and Vulnerability Evaluations (OCTAVE) A process document that provides an extensive risk assessment format (www.cert.org/octave).

GAO Information Security Risk Assessment Case studies of organizations that implemented risk assessment programs (www.gao.gov/special.pubs/ai99139.pdf).

Continued

RiskWatch Software created that poses a series of questions to help individuals perform a risk assessment. It also includes modules for review against the ISO 17799 standard (www.riskwatch.com).

Consultative, Objective and Bi-functional Risk Analysis A risk assessment software program that includes questions that map against the ISO 17799 standard (www.security-risk-analysis.com/index.htm).

Incident response

As we step through the assessment activities, we'll also discuss best practices so that when you're ready to develop your operational security project plan, you'll have the information you need to develop a solid incident response plan. Before we head into the details, let's take a quick look at the history of incident response. This will give you a bit of perspective and it's a great (geeky) conversation starter at tech conventions and high school reunions.

In 1988, an "Internet worm" hit a lot of computers then connected to the Internet. While 1988 may seem like the Stone Age of the Internet, that first attack disabled a large percentage of those 60,000 computers. In response to that incident, the Computer Emergency Response Team (CERT) was formed. CERT was chartered to be a single, trusted point of contact for computer emergency response data; to act as a clearinghouse for trusted information. In 1995, according to the CERT website, there were 171 vulnerabilities reported to CERT. In 2005, there were 5,990 vulnerabilities reported. If the remainder of 2006 tracks with first quarter results, CERT will log over 6,388 reported vulnerabilities. Clearly, we are on an unfortunate upward trajectory.

Those 60,000 computers connected to the Internet pale in comparison to the some-200 million hosts now estimated to be connected to the Internet. It's no surprise, then, that the volume of vulnerabilities reported has increased significantly. Today, there are numerous resources available to anyone who wants to form a security response team and there are also various organizations including the Forum of Incident Response and Security Teams (FIRST) and the TERENA-sponsored TF-CSIRT, a task force for the collaboration of incident response teams in Europe. If you're interested in these topics, visit the CERT site at www.cert.org.

Most organizations don't plan for incident response until after they've had their first incident. This leaves most organizations without even basic knowledge about their network status, such as:

- Not knowing if, for how long, or to what degree the network has been breached
- Not knowing what information has been stolen, modified or corrupted by the breach and the criticality/sensitivity of that information
- Not knowing what method(s) the intruder(s) used to gain access to the network
- Not knowing how to stop a breach in progress
- Not knowing who should respond and in what manner
- Not knowing who has the authority to respond
- Not knowing who to contact regarding the breach (executives, legal counsel, law enforcement)

These problems are amplified by companies with offices in multiple locations, whether domestic or international. Without a clearly defined plan in place, you're putting your company's future at risk. Many companies hold mistaken beliefs about forming an incident handling team. The reasons run the gamut, but here are a few common attitudes that get some companies in trouble:

- It's too intimidating; ignore it and it will go away.
- Just take care of problems as they arise.
- Our firewall keeps us safe.
- It's too much money to spend on something as non-strategic as the network.
- Dave's pretty good with computers, he'll handle it.

Clearly, being in a state of denial doesn't fix the problem, so part of your job is to advocate for the creation and support of an incident response team. This should be one of the major components of your IT operational security project plan, so let's take a look at the details of what that type of team should do and how to form one.

Company-Wide Incident Response Teams

Most organizations of any size and geographic distribution found themselves hastily developing interdepartmental response procedures in the spring of 1999. As the *Melissa* virus knocked out the core communication medium, the bridge lines went up and calls went out to IT managers of offices all over the world. United in a single goal, restoring business as usual, companies that previously had no formal incident response planning spontaneously created a corporate incident response team. Most of the development of formal incident response teams came about as a solution to problems they had faced in managing their response to the most recent issue.

The biggest obstacle in the opening hours of March 26, 1999, was the rapid loss of e-mail communication. Initial responses by most messaging groups upon detecting the virus was to shut down Internet mail gateways, leaving internal message transfer agents enabled. However, it quickly became clear that having already entered the internal network and hijacking distribution lists, it was necessary to bring down e-mail entirely. Unfortunately, security administrators were no different than any other users, and relied almost entirely on their e-mail clients' address books for locating contact information for company personnel. With the corporate messaging servers down, initial contact had to be performed through contact spidering, or simply waiting for the phone to ring at the corporate help desk.

There was a common thread in companies that had difficulty getting back online, even after having gotten all the necessary representatives on a conference call. In most of these organizations, despite having all the right contacts available, there was still contention over responsibilities. In some cases, IT teams from remote organizations were reluctant to take the necessary steps to secure their environments, insisting that the central IT group should be responsible for managing matters pertaining to organizational security. In other cases, the messaging group refused to bring up remote sites until those sites could provide documentation showing that all desktops at the site had been updated with the latest anti-virus software. Clearly, when no one is in charge and no plan is in place, chaos reigns.

Each member of an incident response team should have a clearly defined circle of responsibility. These circles should be directly related to the member's position in an organizational chart, with the relevant corporate hierarchies providing the incident response team's chain of command. At the top of the chart, where an organizational diagram would reflect corporate headquarters, sits the CIO, CSO, or Director of Information Security. The chart should continue down in a multi-tier format, with remote offices at the bottom of the chart. For example, the team member from corporate IT who acts as liaison to the distributed retail locations would be responsible for ensuring that the proper steps are being taken at each of the retail locations.

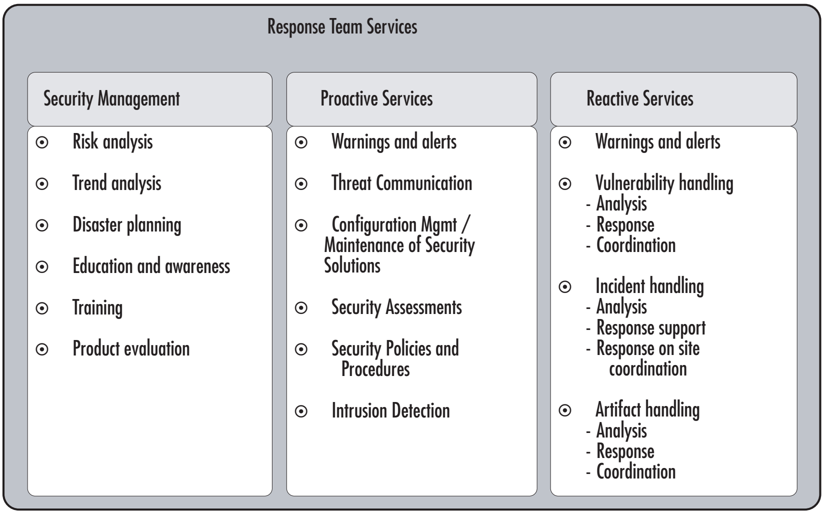
It is important to keep in mind that incident response could require the skills of any of four different specialties: *networking*, *messaging*, *desktop*, and *server* support. At each of the upper levels of the hierarchy there should be representatives, preferably subject matter experts, in each specialty. By ensuring that each of these specialties is properly represented on a response team, you should be prepared to deal with any emergency, no matter what aspect of your infrastructure is initially impacted.

Once the team is developed, you have to find a way to *maintain* the team. At one company, the Director of Information Security instituted a plan to run a fire drill twice a year, setting off an alarm and seeing how long it took for all the core team members to join the call. After the call, each of the primary contacts was asked to submit updated contact sheets, since the fire drill frequently identified personnel changes that would have otherwise gone unnoticed. Another company decided to dual-purpose the organizational incident response team as an information security steering committee. Quarterly meetings were held at corporate headquarters and video conferencing was used to allow remote locations to join in. At each meeting, roundtable discussions were held to review the status of various projects and identify any issues that team members were concerned about. To keep the meeting interesting, vendors or industry professionals were invited to give presentations on various topics. By developing and maintaining an incident response team in this way, your organization will be able to take advantage of the best talents and ideas of your entire organization, both during emergencies and normal day-to-day operations. Properly developed and maintained, this team can save your organization both time and money when the next worst-case scenario finds its way into your environment.

Response Team Services

Although we used the term "incident response" in the section heading, we really should use a broader term, *incident handling*, to indicate what the plan should incorporate. We'll also use the term "operational response team" or "response team" (RT) just so we don't step on any toes (some response team names are trademarked). The response team should be a part of the IT team, but it should also include other key stakeholders such as corporate executives, facilities and operations management and others needed to handle security incidents. Figure 13.1 provides a general list of services a response team can provide to an organization.

Figure 13.1 Common Response Team Services



Response Team Services

Security Management

- Risk analysis
- Trend analysis
- Disaster planning
- Education and awareness
- Training
- Product evaluation

Proactive Services

- Warnings and alerts
- Threat Communication
- Configuration Mgmt / Maintenance of Security Solutions
- Security Assessments
- Security Policies and Procedures
- Intrusion Detection

Reactive Services

- Warnings and alerts
- Vulnerability handling
  - Analysis
  - Response
  - Coordination
- Incident handling
  - Analysis
  - Response support
  - Response on site coordination
- Artifact handling
  - Analysis
  - Response
  - Coordination

Security management includes performing a risk analysis, which is part of the IT security projects we've discussed throughout this book. Trend analysis can also be part of the security management services. Trend analysis involves looking at network data and analyzing it to search for patterns that occur over time. There's an excellent resource available on trend analysis called *Models of Information Security Trend Analysis* by Tim Shimeall, Ph.D. and Phil Williams, Ph.D. from CERT Analysis Center, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, Penn. It can be found at www.cert.org/archive/pdf/info-security.pdf and is a great reference if you're interested in learning more about the intricacies of trend analysis in the IT security arena. Clearly, someone needs to look at security-related data in log files and elsewhere and try to decipher normal patterns from abnormal patterns that might indicate a problem in progress. Trend analysis might also be part of artifact handling when looking at the trail left by a breach. Disaster planning, which we'll discuss later in this chapter, is another management service the RT can provide. User education is an often overlooked function and assigning this to the RT can keep their skills up-to-date and can provide an extremely useful link back into the user community. In concert with education and awareness, the RT team can provide security training or train-the-trainer programs to ensure that security education is replicated across the enterprise in an effective and efficient manner. User awareness is a critical component of overall network security, and providing consistent, helpful information to users can increase awareness and compliance with security policies and procedures. Finally, the RT can assist in evaluating products for the network. The team might evaluate the security features of a new application or the features of a new security product and how, or even if, it might fit into your overall security strategy.

Proactive services include warnings and alerts about threats and vulnerabilities that exist. This is particularly helpful as part of user awareness and education. If users know that a new phishing scam is asking for usernames and passwords, for example, the RT can alert users and help avoid incidents. Threat communication can include technical information being communicated to executives or IT staff. You can task your RT with alerting your IT staff to new or developing threats along with recommendations on how to avoid or address vulnerabilities related to these threats. The team may also be involved with configuring and maintaining security solutions the company is implementing. Configuration management is an on-going security process that should be incorporated into the mission of the RT or should be specifically assigned to a senior IT staff member (or team). Configuration management (CM) ensures that network components are and continue to be properly configured to maintain security. After your security project teams have completed their work, the maintenance of the network configuration should be clearly delegated to an individual or team. In many organizations, this is a subset of the RT. An in-depth look at configuration management is outside the scope of this book, but there are numerous online resources at your disposal to learn more about configuration management and associated software tools you can utilize to assist in your CM processes. The team may be tasked with staying up to date on these systems so they provide the subject matter expertise needed to manage these security solutions at optimal levels for your organization.

Reactive services are, of course, the ones you hope you'll never need. Should your organization have the need for an incident response, a rapid deployment of your RT can make all the difference between a 'simple' intrusion and a devastating breach. The reactive services provided by the RT can include warnings and alerts about threats or intrusions that appear to be occurring (during initial assessment) or that actually are occurring (initial response). They can handle vulnerabilities including analysis, response and coordination. When vendors or other industry experts announce newly discovered vulnerabilities, you need a team that can rapidly assess the organization's exposure and respond with recommendations, procedures, patches or monitoring services to address the specific vulnerability. If an incident does occur, they are typically the first responders who will analyze the problem, coordinate efforts across the enterprise to respond to the problem and provide response services on site, if that's the stated function of the team. In some companies, an RT deploys to the various company locations to coordinate incident response.

In other companies, the RT is centrally located and provides e-mail and phone support to widely-dispersed IT resources domestically or internationally. Finally, the reactive services include handling what are commonly called "artifacts" in the computer forensics field. It's estimated that over 85 percent of all cybercrimes leave an electronic trail, or an electronic *artifact*. The term artifact is usually used to connote "of human craft or invention," so artifacts of cybercrimes are those electronic trails or footprints left by the intruder. The RT should be trained in finding, analyzing and responding to the artifacts found in the wake of an intrusion attempt or a breach.

Business Intelligence…

Computer Security Incident Response Teams

Computer security incident response teams, or CSIRTS, are teams that not only respond to computer security problems; they should be proactively involved with helping your company avoid computer security threats. There are numerous books, articles, white papers and Websites that provide specific guidance on forming and managing a response team. Our goal in this chapter is not to provide you with a step-by-step guide for forming a team, but in assessing your response capabilities, we will cover the basics of an RT. If you'd like more information on forming a world-class incident response team, check out these websites for starters.

Carnegie Mellon University Software Engineering Institute (CMU SEI)- www.cert.org/csirts/csirt_faq.html

Computer Security Institute - www.gocsi.com/

SANS (SysAdmin, Audit, Network, Security) Institute – www.sans.org

Response Team Assessment

We've briefly covered response team services, so let's turn our attention now to your RT assessment. You'll need to take a look at a number of factors as you look at your company's need for a response team. If you already have a team in place, you need to assess the services provided by the team and whether or not the team is covering all the bases. We've continually talked about the three primary components of all security plans: people, process and technology. A response team interacts with all three of these elements in a variety of ways. We know that IT security comes about as a result of a multi-layer defense strategy that includes:

- Keeping operating systems and applications patched and up to date (technology and process).
- Installing, maintaining and monitoring perimeter defenses (technology and process).
- Reviewing, revising and publishing security policies and procedures (people and process).
- Providing security awareness training to users (people and process).
- Managing incidents (people, process and technology).

Using the model we developed earlier, let's look at your response team's capabilities. There is clearly some overlap in these areas with security activities we've discussed in other chapters.

Security Management Services

Risk analysis, disaster planning, user awareness, training and product evaluation all fall under security management services. We've already discussed risk analysis and risk assessment elsewhere in this book, but this is certainly an area that can be part of the RT's mission, either as part of your corporate IT security initiative or as part of the on-going operations after the security initiative is complete. Security is not a one-shot deal, so you will need to have a team dedicated to on-going security assessment, analysis and planning.

Risk Analysis

We've covered risk analysis and assessment throughout this book, so you should have a clear understanding of what skills are required to perform a thorough risk analysis. If your RT doesn't have the skills needed to confidently perform a risk analysis, you have one of two viable options. The first is to send one or more of your IT staff to intensive training to upgrade and update their skills so they can perform a comprehensive risk analysis. If you don't have staff on board that you believe is capable of this, you might need to look at hiring an outside consultant to perform your risk assessment and analysis for you. However, in the long term, you will need this capability on your team, so you should look both near- and long-term at your options.

Trend Analysis

The CERT document referred to earlier on trend analysis provides an excellent explanation of how trend analysis can help improve network security. Authors Shimeall and Williams state, "In the area of information security, enhanced understanding of trends, patterns, and anomalies could contribute significantly to indicators and warning processes that are a key component of efforts to anticipate, thwart, or mitigate intrusions. It is possible, for example, to extrapolate trends so that defenders have at least some expectation about broad developments that might occur. While this is not foolproof by any means, it can provide some basis for anticipation and lessen surprises." Trend analysis should be part of your response team's security management services so that it can potentially anticipate and monitor troublesome trends and avoid being caught completely off-guard.

Disaster Planning

Disaster planning is part of the security services an RT can provide. The RT can develop a thorough disaster plan that should be part of a larger business continuity planning initiative for your company. If disaster were to strike, how would your company continue daily operations? The answer clearly goes far beyond the functionality of the network and the availability of databases and websites. If possible, avoid taking responsibility for the entire business continuity planning process since IT is just one piece of the puzzle. A business continuity project should be headed up or at least sponsored by a senior level executive, and a business continuity planning project should involve stakeholders from every part of your company — facilities management to operations, finance, HR and IT, to name a few. Disaster planning from a business perspective includes how IT services will be re-established after a disaster. Disaster planning from an IT perspective involves how network services will be restored after a disaster occurs, including natural disasters and network security breaches.

Your assessment should look at your RT's capabilities with regard to disaster planning including the existing disaster plan, the ability to manage and implement a disaster plan after a disaster strikes. We'll cover this in more detail later in this chapter.

Education and Awareness

Although adequately managing your network borders can help to prevent a substantial portion of the external threats to your environment, there are always going to be access points that you simply cannot control. Users who bring their laptops home with them can easily provide a roaming target for autonomous threats such as worms, Trojan horses, and other applications that are forbidden by corporate policy. A software update from a vendor might inadvertently contain the next Code Red, as of yet undetected in an inactive state, waiting for a certain date six months in the future. No matter how locked down your network and perimeter may be, there will always be risks and vulnerabilities that must be addressed. Raising user awareness about security threats, risks and vulnerabilities and educating them about how to avoid or reduce these risks is as important as locking down your borders. Developing effective awareness campaigns should be part of the security management responsibilities of your RT team. A review of educational and awareness activities is part of your RT assessment. Awareness campaigns include awareness of security threats, security best practices as well as awareness of corporate security policies. We'll discuss creating security policies later in this chapter, and the awareness techniques we discuss here also apply to policies you and your team develop to address on-going security practices.

Developing Effective Awareness Campaigns

In order to get the attention of the user base, you'll need to provide incentive to the managers of those groups to help IT get the word out about how to recognize and respond to potential security threats. In order to involve the company's managers in IT security, RT leaders have to make the tasks as simple as possible. When the guidelines are clear and concise and leave no room for interpretation, your chances of maintaining security are much higher. There are many examples of fairly straightforward tasks that can be assigned to managers. For example, the enforcement of acceptable-use policies is one of the most common ways to involve management in information security (though the detection of violations is and probably always will be an IT responsibility).

Company-wide awareness campaigns also leave room for engaging management in your information security posture. Although the IT staff can do a lot to protect users from inadvertently causing harm to the company by implementing technology-based safeguards, in many cases, the users are still the last line of defense. If we could magically teach users to never leave their workstations unsecured and to recognize and delete suspicious e-mail, a considerable portion of major security incidents would never come to fruition. Let's look at three common approaches to disseminating security awareness materials. You can assess whether your RT is taking appropriate measures, given your corporate culture and network structure, to raise and maintain user awareness about IT security through:

- Centralized corporate IT department
- Distributed department campaigning
- Enforcement

Creating Awareness via a Centralized Corporate IT Department

Using this approach, corporate IT assumes responsibility for developing and distributing security awareness campaigns. The problem with this approach is that there is an inherent conflict of interest here. Your IT staff is tasked with keeping the network up and running and at the same time, they are asked to lock down the network to keep it secure. Government best practices (National Security Agency, for example) suggest you keep these two functions completely separate. This is not always possible in small organizations, but if you can separate these out, you'll probably have better results. Your organization may already have produced mouse pads, buttons, or posters that include the help-desk telephone number and instructions to contact this number for any computer issues. Sometimes, this task is handed to the messaging group, and periodic company wide e-mails are distributed including information on what to do if you have computer issues.

Depending on the creative forces behind the campaign, this method can have varying results. Typically, such help-desk awareness promotions are fairly passive in nature. When a user has a problem, he or she looks up the help desk e-mail address or phone number or search for the most recent e-mail to find the number of the help-desk. Communications received from corporate IT are often given the same attention as spam—a cursory glance before moving on to the next e-mail. Part of the reason for this is the nature of the e-mail – many users assume it will be too technical to understand. Let's face it, IT departments are not known for their effective communications styles with users. (If your department excels in this area, you're among the elite).

Even plastering offices with posters or mouse pads can be overlooked; people can become immune to any kind of mass communication today. After all, they've learned to look past banner ads, ignore billboards, mute the TV during commercials and skip entire pages in the newspaper. There are numerous methods of effectively communicating with your user base. You can use humor, rewards and awards (some people might consider this a form of corporate bribery, but if it works, it may cost far less than recovering from a security breach) to get users to pay attention. Look for ways to be creatively entertaining. Ask users to submit humorous IT-related anecdotes and include them in your e-mail distribution. Give small awards to those who submit the selected story. Include a little known fact or an amusing quote – anything to get users to actually read IT e-mail on security. Be sure to make the e-mail readable – leave out jargon and complicated explanations and just make it clear, concise and engaging. If you don't have someone on the RT team that can craft this kind of message, collaborate with your internal communications or PR department for some assistance. In the end, the most challenging obstacle in centralized awareness campaigns is actually getting the attention of the user to ensure the information is read, absorbed and retained.

Creating Awareness via a Distributed Departmental Campaign

In some highly compartmentalized organizations, it may be beneficial to distribute the responsibility for security awareness to individual departments. This approach is useful in that it allows the department to fine-tune the messages to be relayed to the users in a manner more aligned with the users in that area. For example, if global messages are deployed that focus heavily on preventing data theft or inadvertent release of proprietary documents, some staff may perceive these e-mails to be irrelevant to them. If they believe the information does not apply to them, they will disregard the e-mail and the information contained within. If a local department is tasked with delivering certain messages, the RT team can work with departments by providing the message and allowing (or requesting) department to tune the message to their department. The upside to this is that the message might be delivered in a manner more appealing to the targeted users. The downside is that your RT will have to be confident that the departments are actually distributing the message. It certainly doesn't help if your organization has pockets of security and pockets of happy-go-lucky ignorant users because their department never passed the message along. If the responsibility is delegated and never executed, you are in a worse position than if you'd used a centralized IT method of disseminating this information.

In many cases, departmental assistance supplements the centralized security campaign. Issues that can impact users regardless of department are left to IT to manage; more specific concerns such as data privacy and integrity can sometimes be delegated to the organizational groups that require specialized security. The problem is often that departments don't know what to ask and IT doesn't advise. The communication gap at this point becomes the security breach. The response team's charter might include communicating with departmental representatives to identify security needs unique to those areas. This removes the circular problem that often accompanies user security issues – the users don't know the right questions to ask and the IT staff doesn't know what the users need.

The development of such programs will vary greatly from one organization to the next, but as with any interdepartmental initiative, the first task is to enlist the help of the senior management of your department. Once you convince them of the potential benefits of distributing the load of user education, they should be more willing to help you craft a project plan, identify the departments most in need of such programs, and facilitate the interdepartmental communication to get the program off the ground.

Business Intelligence…

USB Sure Is Handy, but Consumer Keys Are Creating a Huge Security Headache

USB makes it extremely convenient for employees to transfer data to portable devices, whether it's for work at home or more sinister purposes. It's not easy to deal with the security headaches this practice creates, but tools are now emerging that allow administrators to know which external devices have been connected to the network, and which files were written to them. Typically this is accomplished with software agents that allow network managers to centrally control USB devices. One approach is to enable the use of company-issued USB drives, while rejecting others. Both SanDisk and Sony have created USB devices that use biometric (fingerprint) technology to secure both a computer (desktop or laptop) and the USB device itself.

Creating Awareness via Enforcement

In a pure enforcement awareness campaign, you count on feedback from automated defense systems to provide awareness back to your user base. A prime example is a content filter scheme that responds to forbidden requests with a customized message designed not only to inform the user that their request has been denied, but also to remind the user that when using corporate resources, their activity is subject to scrutiny. This approach can be quite effective, but there is the potential for this method to backfire.

In many organizations, IT is viewed in any one of several potentially negative ways. The "Enforcer" image usually doesn't foster good will and cooperation between IT and users. If IT takes on an adversarial role, the users are not likely to willingly comply with IT requests or mandates unless they have no other option. In any kind of management relationship, developing the desire to cooperate is always more effective than forcing someone to do so. If users have a dislike or mistrust of the IT department or the RT, they're likely to ignore a virus warning or fail to notify IT of a strange dialog box that popped up after they clicked on a link in an e-mail.

There is an element of psychology involved in designing awareness campaigns. Your task is to provide a balance — effectively conveying what users can do to help minimize the various risks to an organization, reminding them of their responsibilities as a corporate network user, and encouraging them to ask for help when they need it. The threat of repercussions should be saved for the most egregious offenders; if a user has reached the point where he or she needs stronger action, it's probably time to recommend disciplinary action anyway. We'll discuss policies and procedures that will help reinforce (and require) appropriate security procedures later in this chapter. Reminding users of these policies and procedures through awareness campaigns can be helpful since most users glance at policies and procedures during their new hire orientation and never look at them again. Keeping them in front of users in a friendly, useful manner can raise security levels significantly. This job falls to the RT in many companies, assuming a company has a response team.

Make certain that users are aware of what they can do to help protect company resources. If a user in your organization suspected that they might have just released a virus, what should they do? Do they know who to call? More importantly, would they be afraid to call? Your RT's job is to make sure users are aware of their roles and responsibilities in maintaining network security.

Policies

Your IT operations security project plan should include a review of your company's current security policy environment. Once you've completed your review or assessment, you'll need to create a project plan to revise the corporate security policies to help support and enhance network security after your project work is complete. In this section, we'll break down the process into several defined steps, each of which help you to create, review, and enforce the policies you need to secure your corporate network. As we've discussed, current technology can be used to *create* a secure infrastructure, but good policies are necessary to *maintain* it.

Security policies are usually seen as necessary to gain compliance with some higher authority, not as a needed function in network operations. They are often overlooked and undervalued until they are really needed. People, unlike computers, don't follow instructions exactly as told. They have choices, and their choices can put cracks in the security walls. Based on research conducted in 2002, about 78 percent of internally caused security breaches were due to inadequate security policies or users disregarding those policies. The question is: Why weren't security policies put in place if they could have helped to prevent some of these incidents? Part of the answer is that companies may not be aware of just how much security policies can bolster network security.

Founding Principles of a Good Security Policy

A security policy will not solve all your misconfiguration and personnel problems, but it will provide a piece of the puzzle that no other component can provide: structure. Clearly, the goal of information security is to maintain information confidentiality, integrity, and availability (CIA). Security policies are one of the few security tools that help us guard against unknown, unforeseen, future attacks. Policies define what actions need to be taken to maintain secure networks, such as removing inactive users, monitoring firewall activity, and maintaining current, standard server builds. However, proper policies are also not the silver bullet. Policies that are not reviewed, updated, circulated, or enforced will become outdated and ineffectual.

Security policy is one area where management support is critical. Because security policies deal much more with the day-to-day actions of employees, and changes in policy should ideally result in changes in procedures, it is important that security implementers have the backing of management. Effecting procedural change in a corporation where employees are set in their ways can be very difficult, and requires much effort. Before you make an effort to implement any policies, make certain you have specific commitments from management as to their role in your initiative, and the support they will provide.

Security policies should be clear and concise. We've all read policies that sounded like the attorneys had spent three months on it. While there may be some required "legal language" in security policies, the general rule is that they should speak directly to the target audience and provide meaningful information. There are a number of best practices for writing policies; we've included some of them here as a guide for your policy review. Remember, your review of policies should include not only the actual impact of the policy (the do's and don'ts) but the clarity and consistency of the language. If one policy talks about hosts (which, by the way, is something most users don't understand) and another discusses desktop computers, users may be confused. Review your policies for content and style (this is one place where style actually does count). Here are some best practices to consider:

1. Consider the reader.
2. Use consistent naming conventions.
3. Use an easy-to-read writing style.
4. Keep documents current.
5. Balance protection and productivity.
6. Designate policy ownership.

Understanding Current Policy Standards

There are numerous policy standards you can use as reference points for developing your security standards. We'll discuss a few of them here and you can follow up with some independent research to find out what might be most appropriate for your organization.

ISO 17799

One of the most widely accepted and endorsed security policy guidelines in use is the International Organization for Standardization (ISO) 17799:2000.This document was originally the British Standard (BS) 7799, and was submitted to the ISO in late 2000.

There has been some confusion over the ISO 17799 in that you cannot become certified as ISO17799-compliant. When the BS 7799 was originally submitted, BSI declined to include BS 7799-2 for approval, which is a checklist of controls that a company can be audited against. The ISO 17799 is not appropriate to be certified against, and therefore, the ISO has not offered a certification through its registrars. However, if your company has a desire to be certified against the BS 7799-2, which is the closest certification available, you can get more information at BSI's homepage, www.bsi.com.

The ISO17799 can be purchased from BSI for under $200, and it is a worthwhile investment.Though not perfect, it is one of the best we have, and one of the most widely referred-to security documents. It appears to have good traction and is gaining ground, both in the American and international communities, as a solid security standard.

Business Intelligence…

ISO 17799 – Security Management Guidelines

You may be familiar with the International Organization for Standardization (ISO). In 2005, they released a specification, ISO/IEC 17799:2005, which establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization. According to the website (www.iso.org), "the objectives outlined provide general guidance on the commonly-accepted goals of information security management. ISO/IEC 17799:2005 contains best practices of control objectives and controls in the following areas of information security management:

- Security policy
- Organization of information security
- Asset management
- Human resources security
- Physical and environmental security
- Communications and operations management
- Access control
- Information systems acquisition, development and maintenance
- Information security incident management
- Business continuity management
- Compliance

The control objectives and controls in ISO/IEC 17799:2005 are intended to be implemented to meet the requirements identified by a risk assessment. ISO/IEC 17799:2005 is intended as a common basis and practical guideline for developing organizational security standards and effective security management practices, and to help build confidence in inter-organizational activities."

SAS70

The Statement on Auditing Standards (SAS) No. 70, Service Organizations, is a tool available to auditing firms and CPAs to conduct an audit of a company that already has implemented an information security program. The SAS70 does not contain a checklist of security controls, but rather allows an auditing firm to issue a statement of how well a company is adhering to their stated information security policy.

If you have already implemented a security policy based on a standard, such as the ISO 17799, the SAS70 may give your information security program additional credibility. Having more accreditation groups stating that your program gets a "pass" grade doesn't necessarily mean you have a more secure program. However, it can help to make customers happy or meet federal or insurance requirements. Remember that the SAS70 is not appropriate for use as a checklist to create an information security policy.

There are three other sets of guidelines that might be of interest to you. They are:

- **Control Objectives for Information and (Related) Technology (CobiT)** A free set of guidelines for information security published by the Information Systems Audit and Control Association (ISACA).
- **ISO 15408/Common Criteria** A technical standard published by the ISO used to support the specification and technical evaluation of IT security features in products.
- **Government Information Security Reform Act (GISRA)** Requires civilian Federal Agencies to examine the adequacy of their information security policies, among other requirements.

Business Intelligence…

Guard Against the Unknown

Imagine if you were able to stop attacks before they started. Imagine if you were able to patch vulnerabilities before they are discovered. Sound impossible? Perhaps not.

If you implement proper information security policies and procedures, you may be able to prevent attacks before they even start. For example, if your policies require you to follow the principle of defense-in-depth, and you have a properly implemented security perimeter around your entire network, you are less likely to suffer an impact from a failure in one component of your network. Another example: If you have proper personnel policies and procedures implemented, such as performing background checks on employees, removing old user accounts held by former employees, and evaluating the threat potential of current employees, you may be less likely to suffer an attack from an insider. With the proper personnel controls in place, you may be able to recognize and mitigate threats from a potentially subversive employee before they take action. You may even be able to recognize them as a threat before they get any ideas and address the problem before it starts.

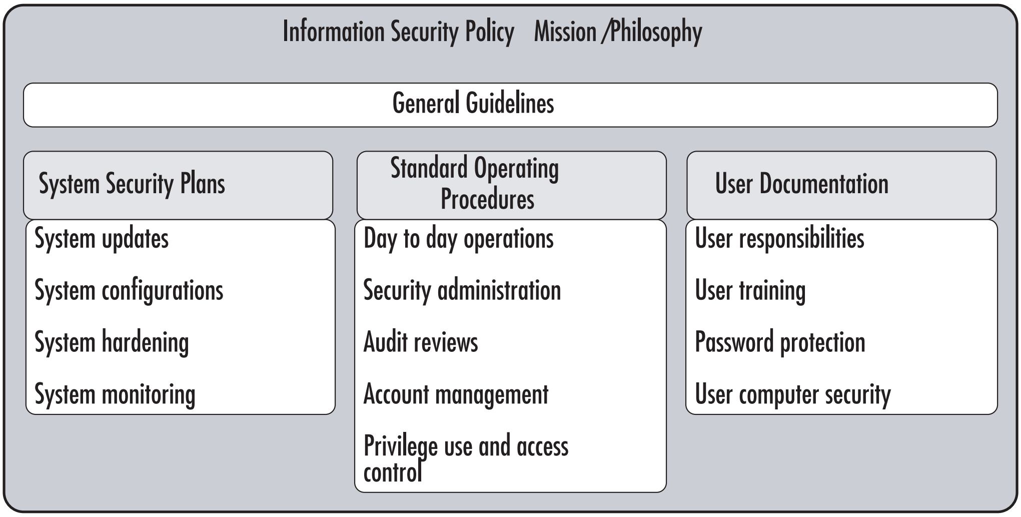
Creating Corporate Security Policies

Let's begin by stating something obvious, but something easily overlooked. Policies include the written policies in your employee handbook and they also include computer-related methods of managing network security. Both types of policies interact, but they are managed in two distinctly different ways. A written policy can be developed from a software program, replicated throughout the organization and enforced through monitoring user behaviors. A computer policy is developed on the computer, replicated throughout the organization and enforced using hardware and software tools. In this section, we'll discuss both kinds of policies. Let's begin with "written" policies.

First, gather all existing corporate policies that pertain in any way to computer or network security or to security, in general. You want to include general security policies because some may tangentially relate to network security such as policies regarding visitor access or after-hours access to the premises. These kinds of policies clearly impact the overall security of the network and should be included in your scope. The scope for policy review and revision should be "policies that directly or indirectly impact the security of the network, the confidentiality, integrity and availability of the data on the network and the users who use the network." While that's a broad statement, you should start broad and narrow it down later, if needed.

Almost all procedures require technical insight into some area, and many procedures should not be developed without input from experts in those areas. Even areas such as physical security require insight into physical authentication routines, biometrics, and networking and power considerations for physical setting of systems. On the other hand, an exclusive focus on the technical elements may miss some of the people-side issues, which is why you want to have a wide representation of stakeholders participate in these policy review and revision tasks. Figure 13.2 provides a framework, based on the NSA model, of how security policies and procedures should be laid out.

Figure 13.2 Framework for Security Policies



Once you've identified all existing corporate policies that fall within your stated scope, you should categorize them if they are not already categorized. There are numerous resources you can use in creating policies, and if you plan on using a resource (book, manual or software program), you may want to utilize the categories provided. Remember, you may have written computer policies that address these areas. Using the model provided in Figure 13.2, we would say that our written policies fall into the "User Documentation" category and our computer policies fall into the "System Security Plans" category. For example, your written e-mail policy might state that users are not to click on links provided in e-mails from unknown sources. Your computer e-mail policy might prevent users from downloading images in e-mails automatically. Both are e-mail policies; both are implemented in different ways for the same intended effect – network security. We've included a list for your reference, and while it doesn't cover every possible topic, it's pretty extensive.

- Anti-Virus Process
- E-mail Policy
- E-mail Retention
- Encryption Policy
- Information Sensitivity Policy
- Internet DMZ Equipment Policy
- Password Protection Policy
- Remote Access Policy
- Server Security Policy
- Use Policy
- VPN Security Policy
- Wireless Communication Policy

You can also head up to the SANS website for a list found at www.sans.org/resources/policies/#template and download either

Microsoft Word formatted document or Adobe PDF formatted files. These are templates you can use by inserting your company's name in them, so they can be very helpful. You can also review the various security checklists provided by the National Institute of Standards and Technology (NIST) and review the policies required to address all of these various security areas. The checklists can be found at http://csrc.nist.gov/pcig/cig.html.

However, there are four things to keep in mind when using templates.

1. Templates are *one-size-fits-all* and may not be right for your company. You may need to edit them or revise them pretty significantly to make them fit your situation, so don't just do the old "cut-and-paste" and hope for the best. Review, revise and edit until the policy fits your environment.
2. If you do use templates, be sure that they fit your organization's overall tone and approach and that the resulting policies are clear, concise and user-friendly.
3. Be sure that you have the legal right to use the material. You don't want to inadvertently use copyrighted or protected material inappropriately. Most templates indicate how and when they can be legally used and they usually include internal use, but you couldn't sell the templates as your own, for example. Be sure you're in the clear when using templates or language from other sources.
4. Check the final draft with your Human Resources department, your executive team and your legal counsel before finalizing and releasing them. There may be issues about which your team is not aware that should be incorporated into your policies, especially if you use templates that originate outside your organization.

Your policy team should include representatives from legal, human resources, management and IT staff. The security policies should include or address these high level issues:

- Acceptable-use policies
- Permitted activities
- Discipline or repercussions for infractions
- Auditing policies
- Disaster recovery plans
- Reporting hierarchy and escalation paths
- Overall security policy
    - What needs protection and from what type of attack?
    - What methodologies will be utilized for protection?
    - Who is responsible for implementation, monitoring and maintenance?
    - Risk analysis – what is vulnerable and what is the cost if lost/damaged/compromised?
- Growth and service needs projections
- User training and education plans

These documents are necessary for the proper implementation and enforcement of policy after delivery of your overall security plan and your RT may be the team responsible for these activities. One thing should be clear is that these activities should be someone's responsibility, and it should be clearly stated in the job description so that one person is the primary owner of these activities. Otherwise, you risk having no one in charge and that's a sure recipe for failure.

Policy development, like IT security management, is a process. It contains a series of steps that takes the user towards a goal, and no single fix can solve all problems. The following is a process that draws from multiple resources to help security managers develop their policy:

1. **Justification** Formalize a justification for the creation of your security policy. This usually comes from a management directive, hopefully from the Board of Directors. This is your ticket to

create what you need to get your job done. Make certain you have a way to check back with the Board or executive team should it be necessary to get organizational support to complete the task.

2. **Scope** Clearly define the scope of your document — who is covered under your policy and who isn't. Does this apply to all users, to mobile users, or just to Help Desk staff? Does this apply to data centers, to remote offices or to all locations? Does this policy apply to company employees and contractors as well as external vendors? Be as clear and exact here as possible because as with any scope statement, this defines the boundaries. It might also be helpful to define what or who a policy does not cover. If this applies to data centers but not to vendors' data centers, state that clearly. Some topics useful in defining scope are:

- Data centers
- Subsidiaries
- Customer call centers
- Satellite offices
- Business partners
- Professional relationships
- Clients
- Suppliers
- Employees, contractors and vendor staff
- Salaried versus hourly employees
- Executive versus non-executive staff
- IT security staff or management versus IT operational staff

3. **Outline** Compose a rough outline of all the areas you need your policy to cover. If you start here, you'll be able to fill in the blanks as you find sample policies, omit redundancies, and create controls to enforce your policies.
4. **Management support** Management support is different from justification. Justification says "we need this done, and this is why." Management support says "I will help you get this done." This usually comes in the form of support from VPs for smaller organizations, or department managers for larger organizations. Having the support of the Board behind you can make this task much easier.
5. **Areas of responsibility** This is related to the initial scoping you performed, but on a more detailed level. By now you have identified the general areas where you will be responsible for creating a security policy. For example, in your scoping you may have defined that your policy will cover data centers that are directly controlled by your organization, not third parties. You may also have already contacted the manager for the data center and informed them that you will be creating their security policy. If physical security is already covered under a corporate physical security policy, and the data center follows these policies, it may not be necessary to create a second, redundant physical security policy. However, you certainly could integrate the current physical security policy into your document, and include any modifications if necessary, so long as you have permission of the physical security policy coordinator.
6. **Implementation and Enforcement** Once the policy is written, the easy part is over. Distributing it to the rest of your organization, and ensuring it is read and followed, is the hard part. This is one of the most critical steps in developing your policy program. This is where all your work culminates in getting results and is one of the most important reasons to have management support. If you have managed your program properly, there

are many managers, plus the Board, that have supported you in your policy development process. Hopefully you have maintained good relationships with all of them, and they are anticipating the final result of your work. If you write your policies correctly, they will not be an additional burden on your users and there will be less resistance.

7. **Review** Once you have developed and deployed your policy, your job is not yet finished. Changes in regulations, environment, business strategy, structure, or organization, personnel, and technology can all affect the way your policy is interpreted and implemented. Remember that policies should be living documents and the responsibility for maintaining these policies can be delegated to your RT or to a sub-team whose mission is to review, revise and maintain security policies. This is especially true in corporate environments in which you must comply with regulatory or legal standards.

There are also a number of free or commercial policy templates, some of which are listed in this chapter. With the acceptance of the BS 7799 as the ISO 17799, there is a worldwide standard on which you can base your policy creation decisions. However, many policies in existence today were not created using guidelines or templates, but were thrown together in an ad hoc fashion. This is why a policy review should be conducted as part of your IT operational security project – to update and revise policies to create a clear, consistent body of knowledge for the organization.

It's helpful if all policies related to IT security follow the same basic format so that users can quickly read and understand the policies. Creating a template for your policies will make the job of creating policies easier, as well. We've listed the headings that are typically found in security policies, and you can use these to craft your own template. These are based on best practices, and you can select the sections that make sense for your organization.

1. **Policy Name and Overview** Give a brief overview of the policy.
2. **Introduction** Introduce the policy, goals, and why it exists.
3. **Purpose** What is it meant to accomplish, and what risks does it mitigate?
4. **Authority** Who approved this policy?
5. **Policy Ownership** Who is the owner of this policy; who makes changes, and who do I contact with questions?
6. **Scope** Where does this apply to the organization, and who is affected?
7. **Duration** What is the time span of this policy's existence?
8. **Related Documents** What other documents contribute to this policy?
9. **Actual Policy Text** What actual rules will be implemented by procedures?
10. **Roles and responsibilities**
    1. Roles defined and assigned to employees for various classifications.
    2. Responsibilities defined for each role.
11. **Compliance requirements** How do you comply with this policy and what constitutes a violation?
12. **Exceptions to this policy** Those explicitly outside scope.
13. **Enforcement of this policy** How is this policy enforced and what are the consequences for violation?
14. **Revision History** Tracks changes; necessary for handing off to new owners.

Tools

There are a variety of tools available that can help you write your information security policies. These are useful if the policy administrator does not have the time or resources to create an information security document. However, be careful to not place too much trust in the prewritten policies. No policies should be created and deployed if they haven't been reviewed for consistency and checked for conflicts with corporate or government regulations.

Charles Woods has developed a well-regarded compilation of security policies, especially ones that can help you with compliance issues. You can learn more about products that help you develop policies and practices that assist in security and compliance at www.informationshield.com/index.htm.

Another product that you might find useful is PolicyCenter, which helps the policy administrator to create their policies and distribute, track, and enforce them. PolicyCenter uses the templates from Wood's Information Security Policies Made Easy. For more information, see www.pentasafe.com or www.netiq.com/solutions/security/default.asp.

NetIQ offerings allow administrators to create, distribute, and enforce their policies. These features help to create a "living policy" document. For more information, visit www.polivec.com.

Business Intelligence...

Rewriting Your Policies for a Management System

With the advent of automated security policy management systems, there are some things you may want to consider when implementing your information security policy. Do you want to backtrack and implement part of your security policy program using an automated tool? Consider the benefits, but also consider the traps. On one hand, you will be able to monitor continuously for compliance with your security policies, checking everything from patch level to password strength, from access controls to

Continued

intrusion signatures. This can assist you in securing your hosts and network by holding the reigns of policy tight on your network.

However, also consider the switching costs involved once you port your existing policies to the new management system. This will take time and resources, and will probably need to be repeated if you choose to switch to a competing product. In addition, these products are relatively new and untested and may have their own inherent concerns. Finally, these products cover only a specific set of information security policy procedural controls and still require the maintenance of a policy administrator.

Consider the needs of your network and whether you feel you will benefit from the implementation of such a system. If your corporate culture or policies require tight maintenance on compliance with policies in your hosts and networks, either due to heightened threats or government regulation, an automated security policy management system may be appropriate. However, if you think it will add to the security of your network, but you fail to implement additional policies and controls, you are probably leaving a gaping hole in your security policy.

Policy Distribution and Education

Now that we have created our policies, either from templates or tools, we need to implement and enforce them. No matter how wonderful and eloquent a policy may be, if it's not distributed and enforced properly, it is not worth the paper it is printed on.

First, we have to determine the scope of our recipients. It won't make much sense to give our new policies to individuals who don't need to read them, and at the same time it would be a mistake if we missed important personnel. The answer is *not* to distribute all policies to all people in a blanket coverage issuance of our new policies. Instead, you should work with your stakeholders to determine which policies should be distributed to the various segments of the user population.

By discussing this with stakeholders, you can provide a useful IT perspective about security while the stakeholder provides a useful perspective about the user community. Striking this balance will help ensure the policies are not only targeted to the right users but that there are no critical gaps. A few overlaps are better than gaps, but a blanket distribution is almost guaranteed to miss the intended target.

There are numerous creative ways to get users to read and implement policies and security guidelines. As much as you might like to just send them out in a long PDF file or email and then post it on an intranet, that technique is number one on the top of the list of ineffective ways to promulgate security policy.

Instead, make the task palatable. Have department managers discuss policies at staff meetings, post important policies on posters in hallways and break rooms, include the important information in bite-sized chunks in newsletters or interesting e-mails or as screensavers or "message of the day." When you make the communication quick, easy and relevant to the intended audience, you're more likely to get a higher rate of compliance.

Remember, you can simply stand there and be the enforcer, which is only effective when you're standing there, or you can gain compliance through education. It's how good managers manage. By educating your audience in interesting and informative ways, you get higher compliance over a longer term than if you stand there ready to handcuff anyone who disobeys. Get your Human Resources and Training teams involved with educating people on the key policies and find ways to keep these messages in front of users in ways that they won't simply overlook. There are numerous resources you can use to create awareness programs,

Here are two useful links for help in creating an effective awareness program:

- http://csrc.nist.gov/ATE/awareness.html
- www.sans.org/rr/whitepapers/awareness/

Maintaining Corporate Security Policies

Policies must be maintained with constant diligence; otherwise, they will become stale and outdated. The more policies become outdated, the more difficult it is to bring them, and the company, back into compliance. A tool has been released by the Human Firewall Council (www.humanfirewall.org), which allows administrators to evaluate their current security practices against the ISO 17799. It also provides them with a Security Management Index, a ranking of their security management against others in their industry.

As you know, a project is a unique solution to a unique problem, but a process or procedure is developed in response to an on-going need. In this case, you're using a project to develop a process, which is a common outcome of project work. Develop a process for reviewing security policies on a periodic basis. If you are subject to compliance or regulatory requirements, you will absolutely need to have a reliable *process* in place for staying up-to-date. If you are not subject to regulatory constraints, you need to implement a periodic review in order to simply maintain network security. Outdated policies can become a legal liability as much as having no policy in place, so don't assume you can create policies once and be done with it.

If you find this entire endeavor to be a bit unappealing (most IT folks would rather go study DOS commands than deal with policies), find someone on your team that finds this interesting and challenging. Find someone who communicates well and (ideally) is a decent writer and ask them to own the process or the task or to head up the project team. This is a very important part of overall network security and it should get your star players, not your also-ran's. Well-crafted policies delivered in an appealing and usable format will go much further than any firewall ever can. Incorporate solid policy development and management as part of your overall operational security plan.

Disaster Recovery

Disaster recovery is often considered a key component of business continuity planning. However, business continuity planning is broader in scope than disaster planning from an IT perspective. Therefore, it's important that your IT disaster recovery plans include other key stakeholders in the organization. Disaster response planning should be a coordinated effort among various groups within the company. Disaster planning and business continuity planning is a big undertaking and will require a concerted effort on your company's part to develop a coherent plan. A thorough discussion of disaster planning is outside the scope of this chapter, so we'll just cover the basics here. You and your team will need to do additional research to determine the specific elements you'll need to address for your company since every company's disaster and business continuity plans will be different. The basic elements of such a plan should include:

1. Examine and analyze potential threats and vulnerabilities
2. Assess impact of a disruption to normal services
1. Alternative business process handling
2. Customer service backup and recovery
3. Administration, operations, communications and IT
3. Prepare information about existing systems
4. Review involvement of emergency services
5. Initial assessment of potential impact of emergency
6. Mobilizing the recovery teams
7. Notifying employees, families and the media
8. Maintaining suitable records and event logs

You'll need to make sure you cover these key areas:

- Facilities
- Hardware and software
- Communications
- Data files
- Customer services
- User operations
- IT network and communication services
- End-user systems
- Other processing operations

There are a variety of books, training courses and tools available on the Internet that will assist you in creating a business continuity and disaster recovery plan for your organization. While this is not solely the responsibility of the IT department, it's unlikely there is another group in your organization that is, or should be, tasked with this job, so you should consider it the job of IT to head up this planning effort.

The Small Business Administration's website provides a number of guidelines that should be considered in your disaster and recovery planning, though it is by no means exhaustive.

Facilities

1. Develop contingency plans to remain in operation if your office, plant, or store is unusable. Could you operate out of your home or a nearby storefront? Could you quickly transport critical items such as computers, inventory, and equipment? Could you save replaced equipment and reactivate it in an emergency? Could you store inventory, equipment, and supplies off-site? Examine the possibilities, make a plan, and assure that you and your employees know what to do.
2. Keep extras of any hard-to-replace parts or supplies on hand. Store them off-site. If this cannot be done, work with suppliers in advance to assure a secure and adequate supply. Store several days' supply in a place that is not vulnerable to the same disaster as your facility. Be sure to keep this auxiliary supply up-to-date.
3. Make upgrades now that would prevent possible future damage. Strengthening exterior walls, adding a retaining wall or shoring up a creek bank are relatively minor projects in comparison to losing the building to flood waters.

Operations

1. Purchase a backup generator to maintain full operations or critical functions such as refrigeration, lighting, security systems, and computer control in the event of a power failure.

2. Have back-up vendors and shippers in place in case your primary ones are disabled. Set up relationships in advance and maintain them. Place occasional orders so that they regard you as an active customer when you need them.
3. Guard against loss of your customer base by diversifying your product lines, sales locations, or target customers. Make it part of your annual plan to develop new customers, even if your current customer base seems fine. Make the time to do so.

Information and Communications

1. Make backup copies of all critical records such as accounting and employee data, as well as customer lists, production formulas, and inventory. Keep a backup copy of your computer's basic operating system, boot files, and critical software. Store a copy of all vital information on-site and a second in a safe off-site location. Make it a critical part of your routine to regularly back up files.
2. Make pre-arrangements with computer vendors to quickly replace damaged vital hardware. Keep invoices, shipping lists, and other documentation of your system configuration off-site so you can quickly order the correct replacement components. Take care of credit checks, purchase accounts and other vendor requirements in advance so that the vendor can ship replacements immediately.
3. Surge-protect all computer and phone equipment through power and phone lines. A power surge through a telephone line can destroy an entire computer through a connected modem. Invest in a surge protector that has a battery backup to assure that systems keep working through blackouts.
4. Maintain an up-to-date copy of phone numbers, computer and Internet logon codes and passwords, employee phone numbers and other critical information in an accessible location. Develop an employee "telephone tree" to rapidly contact employees in an emergency.

Business Insurance

1. Review your current insurance coverage. Is it enough to get your business back in operation? Will it cover the replacement cost of vital facilities? Make it a regular annual procedure to review and update insurance. Also remember that insurance on mortgaged property probably only covers the lender with nothing left over for you.
2. Be aware of your contents insurance. Does it cover the replacement cost of critical equipment?
3. Know what your insurance does not cover. Most general casualty policies do not cover flood damage. Many require additional riders for windstorm, sewer backup, or earth movement. Consider adding coverage for likely perils, especially flood insurance.
4. Consider business interruption insurance that assists you with operating needs during a period of shutdown. It may help you meet payrolls, pay vendors, and purchase inventory until you are in full operation again. Also be prepared for the extraordinary costs of a disaster such as leasing temporary equipment, restoring lost data, and hiring temporary workers.
5. Don't assume that, just because it never happened before, it never will. Flooding patterns are changed by development: water, which runs off new streets and parking lots, may overwhelm nearby streams and surrounding land. Landslides and sinkholes may develop because of distant earth movement, natural or man-made. The creek by your building may be a tiny, placid stream that has never flooded, but a downpour may change it into a destructive torrent that destroys your building foundation. Plan for the worst.

For more information on small business continuity planning and other small business resources, you can visit the Small Business Administration website at www.sba.gov. You can also find some helpful resources on the Disaster Recovery Journal Website at www.drj.com. The information provided here and supplemented by additional targeted resources should spark thought about what your company will need to recover from a disaster, whether that's a security breach or a hurricane, flood or earthquake.

Be sure you put your plan to the test through simulations and assessments. An untested plan is a big unknown and while you can't always simulate everything that will occur during a disaster, you can anticipate the common scenarios and test your plan. For example, if the corporate network was down, you couldn't use e-mail. How would you communicate? What if the phone systems were also out? You might be able to use cell phones if the land lines were down. Simulating a scenario where power, network and phone communications are down might help you identify gaps in your plan. While you may never know how well you've prepared until you need to implement your plan, recent events such as the Hurricane Katrina disaster response have yielded a lot of new information about how to respond (and how *not* to respond) that you can and should use to reinforce your disaster planning activities.

You will likely want to create a separate project plan for disaster and business continuity planning and work through it as you would any other IT project plan. However, this should be part of the mission and responsibility of your response team.

Regulatory Issues

One of the odd things about regulatory and compliance issues is that meeting these standards does not necessarily make your network or data secure. While that is the intent of these kinds of regulations, they often fall short of their intended effect. In part, that's because lawmakers are not IT security experts, and in part, it's because these are complex issues and it usually takes a few iterations before regulations align with the legitimate operational needs of the business. So, don't be lulled into a false sense of security, thinking that if you are compliant, you are also secure.

Earlier in the book, we discussed the legal implications of many of the regulations facing corporations today. In this chapter, we're going to run through some of these same regulations, but this time with an eye toward operational elements such as creating policies that help you comply. We're providing additional resources, but again, it's important to emphasize that because there are serious consequences to being out of compliance, you should be in close communication with your financial, legal and HR departments during your compliance assessment and implementation work to keep you and your company on the right side of the compliance issue. Also keep in mind that many of these policies and regulations are being updated on a somewhat regular basis, so the links or references might change.

Business Intelligence...

Five Compliance Myths

A white paper released by Symantec entitled "Debunking the Top Five Myths of Compliance" is an interesting read for anyone working on compliance issues in the corporate world. The five myths discussed are:

1. Compliance initiatives don't align with business objectives.
2. Compliance can be solved with a project.
3. Compliance is someone else's problem.
4. IT security is about protecting computers.
5. One security/compliance product can do it all.

The white paper provides a good overview but Myths 1 and 2 are of particular interest. The elements common to all compliance initiatives are those things that align with sound business practices, such as accountability, integrity, custodianship, risk management and standardization. If compliance and security initiatives can be seen as aligned with sound business practices and supporting the long-term success of the company, the perception of compliance-related activities might improve. Granted, there may still be a disconnect between the requirements for compliance and the way your business runs, but seeing compliance as part of sound business practices might help your organization buy into compliance requirements more readily. Myth 2, that compliance can be solved with a project, is also an important take-away. While this book is

Continued

focused on project planning for a variety of security issues, it is clear that operational security, the day-to-day security discussed in this chapter, is how compliance is achieved and maintained. It should be assessed, planned and initially implemented via a project plan, but maintaining compliance requires an on-going commitment with consistent organizational practices in place. This is an important point to understand as you plan your organizational security project so you can be sure the hand-off to daily operations at project completion supports and enhances continued compliance.

The Symantec website has a lot of good information on IT security and compliance, though it naturally is slanted toward their products and solutions. You can find the white paper many places online, but here's one link to it: www.bindview.com/resources/whitepapers/Debunking_WP.pdf (Bindview was acquired by Symantec).

Health Insurance Portability and Accountability Act

The Health Insurance Portability and Accountability Act (HIPAA) was signed into law in 1996. HIPAA came about in response to a need to establish standards for the transfer of patient data among health care providers. This includes health care clearinghouses, health plans, and health care providers who conduct certain financial and administrative transactions electronically. Insurance providers, hospitals, and doctors use a wide array of information systems to store and transfer patient information, and have various claim forms with varying formats, codes, and other details that must be completed for each claim. HIPAA was enacted to simplify the claim process. Privacy and security issues were also addressed in this legislation to protect patient data.

The latest documents including resources to determine if your company must comply with HIPAA standards can be found at www.cms.hhs.gov/HIPAAGenInfo/02_TheHIPAALawandMore.asp#TopOfPage. The guidelines include:

1. **Administrative procedures** Documented practices to establish and enforce security policies

2. **Physical safeguards** Protection of buildings and equipment from natural hazards and intrusions
3. **Technical security services** Processes that protect, control, and monitor information access
4. **Technical security mechanisms** Controls that restrict unauthorized access to data transmitted over a network

There are implementation guides available for purchase at www.wpc-edi.com/hipaa.

By now, you're probably aware of your company's need to be compliant with HIPAA, but if you're new to your job or new to the company, you may want to become more familiar with HIPAA. You might find some useful tips on how to address compliance issues on these Websites.

Gramm-Leach-Bliley Act

On November 12, 1999, President Clinton signed the Financial Modernization Act, commonly known as the Gramm-Leach-Bliley Act (GLBA). GLBA includes provisions to protect consumers' personal financial information held by financial institutions. There are three principal parts to the privacy requirements: the financial Privacy Rule, Safeguards Rule and pretexting provisions.

The Financial Privacy Rule governs the collection and disclosure of customers' personal financial information by financial institutions. It also applies to companies, whether or not they are financial institutions, who receive such information. An overview of the financial privacy requirements is summarized on the Federal Trade Commission website at www.ftc.gov/bcp/conline/pubs/buspubs/glbshort.htm.

The Safeguards Rule requires all financial institutions to design, implement and maintain safeguards to protect customer information. The Safeguards Rule applies not only to financial institutions that collect information from their own customers, but also to financial institutions "such as credit reporting agencies" that receive customer information from other financial institutions.

The Gramm-Leach-Bliley Act also prohibits "pretexting," the use of false pretenses, including fraudulent statements and impersonation, to obtain consumers' personal financial information, such as bank balances. This law also prohibits the knowing solicitation of others to engage in pretexting. The Commission has been active in bringing cases to halt the operations of companies and individuals that allegedly practice pretexting and sell consumers' financial information. For more information, visit www.ftc.gov/privacy/privacyinitiatives/glbact.html.

Sarbanes-Oxley Act

As you know, Sarbanes-Oxley deals with financial information and it applies to companies that deal with a variety of financial types of data. As with HIPAA, if your company is required to be compliant with SOX, you're probably already painfully aware of this fact and have had to deal with it. Your operational IT security plan should review current and updated compliance data and ensure that your operational plans incorporate methods that support or enhance compliance with SOX. Clearly, many of these regulations continue to undergo modification, often to clarify the intent or implementation of a particular aspect of the regulation.

If you want more information on SOX, the University of Cincinnati College of Law has a great Website that gives you some of the details (a link from the Security and Exchange Commission Website), at www.law.uc.edu/CCL/SOact/toc.html. Due to the complexity of these regulations, you should certainly involve your financial and legal experts in discussions about what's needed to become or remain compliant. If your company is currently compliant, your IT security project might look at ways of reducing the burden of maintaining compliance through the use of appropriate technologies and through the revision and enforcement of security policies.

If you want to really dig in and learn more, there's a wealth of information on the SEC's Website at www.sec.gov/index.htm.

Business Intelligence...

SEC Announces Next Steps for Sarbanes-Oxley Implementation to Help Small Companies

Anyone working at a small public company knows the challenges that SOX compliance brought on. In response to several on-going problems, the SEC issued a press release that speaks directly to changes that should relieve some of the burden on small companies.

On May 17, 2006, the Securities and Exchange Commission took a series of actions it intended to take to improve the implementation of the Section 404 internal control requirements of the Sarbanes-Oxley Act of 2002.

The actions the Commission intended to take included issuing SEC guidance for companies and working with the *Public Company Accounting Oversight Board* (PCAOB) on revisions of its internal control auditing standard. These actions are based on extensive analysis and commentary in recent months from investors, companies, auditors, and others. The actions also included SEC inspections of PCAOB efforts to improve Section 404 oversight and a brief further postponement of the Section 404 requirements for the smallest company filers, although ultimately all public companies will be required to comply with the internal control reporting requirements of Section 404.

If you read the press release carefully (follow the link provided below), you'll notice some interesting language such as "we will take a giant step toward 'getting it right'" and "future guidance will be scalable and responsive to their individual circumstances." This language suggests that the SEC knows that compliance is needed but that many smaller companies are struggling to make sense or to implement these regulations. Given the number of companies subject to SOX and the overwhelming complexity of the rules, this is an important acknowledgement from the SEC and should help companies that are struggling to become compliant even after compliance deadlines have passed.

For more information or to read the entire press release, see www.sec.gov/news/press/2006/2006-75.htm

There are numerous other regulations to which your company may have to apply but these are the "big three" compliance headaches for most companies. In order to incorporate these regulations and compliance requirements into your IT operational security project plan, you'll need to be fairly familiar with the requirements, so the first step would become well-versed in these areas.

Many companies sell products they claim help companies become compliant with a variety of regulations. Clearly, some of these claims are true and some are probably not-so-true. However, before you run out and purchase a variety of these products, you should complete your assessment and create a project plan for gaining and maintaining compliance. Taking an ad hoc approach to purchasing and implementing compliance products will leave you with a patchwork of solutions that may do nothing more than drain your IT budget. If you use the steps delineated throughout this book – define the problem, define the desired outcome, look at potential solutions, look at constraints, assumptions and requirements, and select the most appropriate solution – you'll end up with a much more thorough and consistent solution to your security and compliance needs. As the earlier sidebar pointed out, security and compliance cannot be viewed simply as "projects," they must be seen as on-going activities that are woven into the fabric of corporate operations. However, becoming secure and compliant is often best done through a project plan that has the development of on-going processes and procedures to maintain and enhance security as one of its objectives.

Project Parameters

Now that we've looked at the elements of IT operational security including incident response, policies, disaster recovery and regulatory issues, let's define the problem statement, the mission statement and the project's other parameters. Remember that your operational security planning should begin with forming a core project team that can participate in defining the project parameters from the ground up. Once you've defined the basic project requirements and parameters, you can then modify team membership so that you include needed subject matter experts and other key stakeholders for the project.

We're assuming you know how to do the basic project definition tasks, so we will run through these elements rather quickly with an eye on operational security.

Problem

The essential problem is that technology, alone, cannot protect your network. People need to understand what they can, should and must do to maintain that security. Your organization needs to have a plan for how to respond if something does happen – whether that's a security breach or a disaster. If your company is subject to regulations, you must develop processes, procedures and policies that enable you to remain compliant and to maintain security after project work is complete. So, let's pose three potential problem statements you can use as starting points.

> Our firm is looking into expanding, and part of this expansion would include handling consumer credit card data. If we choose to go this route, we will be required to comply with GLBA regulations. The executive team wants to know what it will take (how much time and money) to become compliant so they can make a decision as to whether they want to begin handling consumer credit card data or not. At present, we are not subject to any regulation and we do not know if our organization is even close to being compliant with GLBA regulations.
>
> Our firm is required to comply with Sarbanes-Oxley, but we are struggling with understanding the rules, regulations and compliance requirements. Since we are a very small firm, the regulatory burden has been significant.
>
> Our firm has been fortunate not to have experienced a security breach, but we do not have a well-thought out approach to responding to an incident, whether natural or manmade.

Mission/Outcome

Your mission statement, often called an outcome statement, is the flip side of your problem statement and you should be able to come up with an outcome statement pretty easily. We'll continue with the three sample problem statements.

> To provide a clear assessment to management of the time and cost required to become compliant with GLBA regulations so the executive team can make an informed decision about the cost/benefit ratio of the proposed transaction.
>
> Taking a fresh look at our current practices using a more methodical project management approach will yield a better strategy for us to get closer to becoming and remaining fully compliant with Sarbanes-Oxley now and in the future.
>
> We will have a clear, concise plan for maintaining security in the event of a security incident, whether natural or man-made. We will know exactly what to do in the event of a problem and will respond in a calm, rational and effective manner.

Solution

We're taking a short cut here because the next step in your process would be to think through all the possible solutions you and your team could come up with and then rank the solutions, identify organizational constraints that would impact solution selection and select a solution. We're assuming you'll do all of that and that you're ready to select your solution. Clearly, the solution must be one that addresses the needs of your particular organization (time, budget, scope) and if needed, the regulatory environment.

Your solution should also encompass the four distinct operational security areas we discussed in this chapter: incident response, policy management, disaster planning and recovery and regulatory compliance. Your solution will form the foundation of your operational security project plan, so we'll assume for our purposes that you are addressing all four areas. The solution statement would look something like this:

> To address these concerns, we will perform an operational risk assessment and form a permanent response team tasked with reviewing, managing and maintaining operational security including incident response, policy management, disaster response and regulatory compliance related to the corporate IT infrastructure and services.

Your solution may vary but the idea is to determine how you will address the problem and the mission or desired/required outcome. You can also develop your three to five top level objectives at this point based on the solution you've identified. We'll expand on these objectives when we create our work breakdown structure later in this chapter.

Scope

As with any project scope statement, you need to define what is and is not included in your project. This scope statement will form the foundation of your Work Breakdown Structure and after you've defined your WBS, you'll come back to your scope statement to see if the two match. If not, you'll have to revise one or the other so that you have consistency throughout your operational security project. Let's look at some of the things that could be included (or excluded) from your scope statement.

- **Incident response** Your operational security plan, at minimum, should include planning for incident response. Best practices dictate forming a response team but if your planning activities suggest a different and more optimal path, incorporate that into your plan.
- **Policy management** Policy management includes the compiling, review, revision and maintenance of all corporate policies related to IT and network security. You may choose to carve this out into a separate project using a different team. Be clear about whether your project includes or excludes policy management. Also define clear boundaries of policy management for project

purposes so you know what is included and excluded from your policy management tasks.

- **Disaster response** This is part of business continuity planning (BCP) and while IT plays an ever increasing role in BCP, you may decide to parse out this work. For example, your company may already have BCP teams or projects in place and you may need to prepare your IT portions and insert them into the larger BC plan. Be clear about what your planning activities include and exclude and how this fits into the larger BCP process at your company.
- **Regulatory compliance** Compliance crosses several major corporate "boundaries" and touches legal, financial, HR, training and IT. If your operational security plan includes regulatory compliance, be specific about which regulations you're addressing and how you'll gain and maintain compliance. If this is going to be delegated to a regulatory project team or a team whose mission is to manage regulatory issues, be clear about that as well. Compliance must be maintained once achieved, so your project plan should include on-going operational procedures that support compliance if compliance is part of your project plan.

Cost

Operational security planning costs can include the cost of purchasing tools, equipment and training resources but most of your cost in a project of this nature is going to be time. The majority of tasks in this project involve gathering, reviewing, revising, disseminating, managing and updating data. If you have a specific budget allocated to this project, make note of it here so you can compare it to the costs you calculate after developing your WBS.

Time

Operational security planning is usually not as time-sensitive as other IT security projects may be. Certainly having a trained response team or well-crafted user security policies are important and should be in place, but securing the infrastructure is usually a first step followed by a review and improvement of operational security. Therefore, you may find that your schedule for operational security is longer because it typically is not as time-sensitive. That doesn't mean you can "back burner" it and expect everything will turn out fine. It should be a priority to perform the tasks in this project to maintain the security your team has worked so hard to achieve through the other projects.

Quality

As we've stated throughout the book, quality is as much a state of mind as it is specific measurable results. In your operational security project plan, quality will include statements and measurements in the following areas:

- **Incident response** Your incident response plan should include metrics about response time and time between response and recovery. It could include quality measurements related to how many incidents were detected and prevented, how many incidents were detected and responded to and how well various systems performed.
- **Policy management** Policy management quality is a bit more difficult to quantify. The goal should be to create and manage policies that are as clear, concise and effective as possible. Metrics might include number of policies reviewed and revised, number of security incidents related to user issues before and after policy revision or the number of awareness campaigns or employees trained through the policy management activities.
- **Disaster response** BCP and disaster response quality should strive to be as complete as possible. A high quality plan will touch on all the major points of BCP. This area may be difficult to determine the quality of the plan in advance of actually using the plan so testing portions of the plan through simulations and

assessments will be an important part of developing a quality disaster response plan.

- **Regulatory compliance** Compliance is an area where there are sometimes very clear measurements and sometimes vague or conflicting requirements for compliance. As the regulatory environment continues to evolve, especially with regard to computer security, it will be important to use as many quantifiable metrics as possible. Your legal liability may well be based upon quality assessments such as percentage of policies compliant with Statute 123 or the number of transactions that fall inside or outside some particular measurement. If there are specific quality measurements included in the regulatory areas you must comply with, be sure to include those in your quality statements and in your technical requirements.

Remember, too, that you need to assign relative priorities to scope, cost, time and quality so that when you're in the middle of managing your project, you know how to make decisions consistent with the priorities of the project and the organization. Define which parameter is least flexible – the one that should not change — no matter what. Then define which parameter is most flexible – the one that can move around to accommodate the other elements. That's not to say that you shouldn't try to meet all four parameters, but that you need to know the relative importance of these factors so you can work your plan. Things always change in a project, and you simply need to know where to "give" and where to hold firm. Run your decisions by your project sponsor and be sure that he or she agrees with your assessment. If you have a disconnect here, you could end up with a major problem down the road.

Functional Requirements

Your functional requirements describe the things that should be part of the project plan, but they do not describe specifically how those requirements will be implemented. Functional requirements in each of the four areas discussed in this chapter may include:

- **Incident response** Your incident response plan should describe exactly what actions should be done in the event of an incident. How those actions are implemented may be described as part of your functional requirements or they may be part of your technical requirements.
- **Policy management** Policy management functional requirements could include the specific categories of policies your operational security plan will address. Functional requirements in this area could also include specific user or organizational requirements for policy that should be included in the project plan so that you describe the full scope of policies to be addressed.
- **Disaster response** Which disaster response activities should be included in your project? Is this part of a larger BCP or will you be incorporating the basic BCP elements into your operational security plan? Define specifically what you will address within the scope of your operational security project plan.
- **Regulatory compliance** What specific regulations is your company required to comply with and what are the areas of compliance required? If you clearly define these functional requirements, developing methods for meeting compliance requirements will be that much less burdensome.

Technical Requirements

The technical requirements for most IT projects are often the easiest to define, but in the case of operational security requirements, the functional requirements may end up being easier to define. Technical requirements should be developed from your functional requirements and should include details on how you will be required to deliver the functional requirements of the project.

- **Incident response** Your technical requirements should describe how you will respond to an incident. In the technical requirements, you should include tools, technologies and timelines that are required or that will support meeting the functional requirements. If you will use specific tools like sniffer tools or IDS/IPS systems, those should be clearly spec'd out in the technical requirements.

- **Policy management** What are the technical requirements for policy management? They might include specific policy development software tools or they might include the required elements of all IT security policies. The technical requirements provide detail on how you will develop the policies in your organization, so they might also include the methods you'll use to collect, store, archive and manage policy revisions. For example, you might define a document management system for version management as part of your policy management technical requirements. Since policies are typically part of the compliance environment as well, you may need to define specific technologies that will be used to meet policy management requirements for compliance purposes.
- **Disaster response** The technical requirements for disaster response may be quite varied since BCP and disaster response may include partial and full recovery requirements. If your company has multiple geographic locations, your technical specifications will vary from a company that has one location. You might define the amount of power a backup generate will need (or your project plan may include tasks to help you define that), the number of users to be supported in a temporary or alternate work location, the amount of network storage required or the specifications for off-site storage of critical network data.
- **Regulatory compliance** Technical requirements for regulatory compliance vary greatly due to the diverse nature of the compliance environment. Specifications that describe how you will meet functional (and regulatory) requirements may include software specifications, audit cycles, monitoring tools and more.

Legal/Compliance Requirements

There may be legal and compliance requirements that don't fit neatly into functional or technical requirements that you may want to clearly delineate in this section. In addition, even if it overlaps a bit, you may find it helpful to articulate the compliance requirements in a separate section so they can be easily found, referred to and updated as needed. It's wise to take whatever advance steps you can to make your compliance process easier and less burdensome on your entire organization. Keeping compliance requirements separate can also help you distinguish between operational plans that you are choosing to implement to improve security versus those you are required to take by an outside organization that ultimately may, or may not, improve security in your organization.

Success Factors

You may choose to include success factors in your requirements planning or you may choose to include it later in your project assumptions section. In either case, you should clearly articulate what it will take for the project to be a success. If those factors are missing or constrained, your project success is at risk. If the success factors are never articulated, you might fail to realize a key component is missing. Once defined, these can be listed as requirements for the project and can be included in risk management planning as well, since a missing success factor puts the project at risk.

Required Skills

The skills needed for an operational security project plan really run the gamut from technical skills to operational management to communication and writing skills and just about everything in between. We've created a preliminary list from which you can start.

- **Technical skills** Networking, systems (servers, hosts), security components (routers, firewalls), administration, operations, applications, databases.

- **Auditing skills** Thoroughness, attention to detail, understanding of auditing/assessment procedures and best practices, documentation, versioning (document management), and archiving.
- **Planning and coordination skills** The operational security plan touches all parts of the organization so the ability to effectively plan cross-departmental activities and the ability to coordinate across the enterprise are important skills for this type of project. In addition, disaster and continuity planning require strong planning and coordination skills as does developing an incident response team.
- **Writing skills** The ability to clearly articulate polices and procedures, incident response procedures, disaster recovery plans and more requires strong writing skills.
- **Communication skills** An operational security project requires the ability to communicate effectively with a variety of stakeholders across the enterprise. The coordination of incident response or disaster response planning (and implementation) requires strong communication skills as does the promulgation of corporate security policies throughout the company.

Personnel Needed

Your operational security project plan will need people from inside and outside your IT department. After identifying your required skills, you'll need to begin looking for the right resources in your organization to assist in this project. Look across your organization for the right people – don't be myopic and look only at IT staff for help with this project. The more you can reach out and involve people from different areas of your company, the better your organizational security planning process will be. You may still need to head this up and keep in on track but you should certainly include a representative cross-section of your company in this process.

Project Processes and Procedures

Project processes and procedures are those needed to run this specific project. We're assuming you have a whole slew of processes and procedures at your disposal from working on other similar projects. So, let's look at which ones might be unique to an operational security project plan.

First, you'll need cross-functional communication and coordination. Whereas other IT projects teams may have included members from other departments, this project *must* include members from across the organization. Do they all use email? For example, some companies have divisions or sections of their companies that are less technical than others. If you have a manufacturing plant, do all the employees there have access to email or an intranet? If not, then disseminating project update or security policies to them may present a different set of issues. Look across the organization and across your proposed team (we'll cover team composition in the next section) and determine the processes and procedures that might work with this diverse population. If some members of the team use Instant Messaging and other members are not IM-enabled, you may have communication problems.

Second, you'll need to test many of your plans in simulation types of settings. For example, you can run a drill for incident response or disaster response but you won't be able to fully simulate all aspects of an actual problem. Your processes and procedures should address this unique need as well. How are problems with drills or simulations addressed? How should be they be documented or escalated? Certainly, you'll need to have well-thought out change management processes that help you revise your project plan based on results from tests. If you find that your project work or your test results are missing the mark, you'll need to have very solid practices in place to manage the process of implementing feedback and change based on project results.

For compliance and regulatory issues, you most likely have to follow very specific mandatory steps, processes and procedures. These should be included as project procedures so that as you work your way through your project you don't have two sets of procedures to follow. You may choose to incorporate them in a way that makes it clear they are part of the regulatory or compliance process so they can be given the attention needed. You'll also need to define the processes and procedures needed once project work is complete to maintain compliance standards. This is usually accomplished by adding one or more tasks in your project plan regarding on-going operations and project hand-off, as discussed earlier in this book.

Project Team

We've touched on this throughout the chapter because we've talked about the far-reaching nature of an operational security project plan. Once you've defined the functional, technical, and regulatory requirements for the project, you've defined what you need to accomplish in the project. By looking at the specific skills needed to accomplish project work, you've essentially defined who you need. Gathering that team together and coordinating those activities will be your biggest challenge for two reasons. First, you'll be interacting with people from all over your organization and coordinating them can simply be a challenging task. Second, not everyone is going to recognize, accept or respond to the authority of an operational security project manager. This is where executive support becomes vital to project success. If you have one of the top executives in your company supporting you and your project's objectives, you should find more organizational cooperation. If needed, your executive support may also include putting a bit of pressure on unruly or unwilling participants to ensure project success.

Gather your project team together and get them fired up about the project by helping them understand the importance of their work on the project and how it supports and enhances the company's efforts. Make sure you introduce everyone present since there may be people who have never worked together before. In large companies, there very well could be people who've never met or even heard of others before this meeting. Develop a team roster and distribute it to all team members. Define roles and responsibilities so that everyone is clear about how the project will proceed and how they will interact with the team. These are all basic IT project management concepts that are not unique to operational security. However, operational security is likely to pull in people from areas of the organization who may not normally interact closely with IT or who have never been involved with this kind of project. Therefore, it's your job as project manager to pull these folks in, make them feel welcomed and set clear expectations so everyone can work effectively in their assigned roles.

Project Organization

Organizing an operational security project is challenging because it can (and usually is) so wide-reaching in scope. Your typical organizational methods will probably work well but you'll need to coordinate to a greater extent. This type of project lends itself well to creating sub-teams since developing policies is a set of tasks distinctly separate (though related) from forming a disaster response plan. These teams can be coordinated but allowed to work in parallel if the project is well-organized. You may choose to break the four topic areas we've discussed (incident response, policy management, disaster response and compliance) into four sub-projects that roll up into a master plan so that resources, schedules and activities can be effectively coordinated. It's highly likely that you'll have activities that intersect that need to be coordinated. For example, you'll certainly need to coordinate compliance activities with policy development so that the policy team can create the policies and operational procedures needed to maintain compliance on a moving-forward basis. You should also keep an eye on translating all of this work into on-going operational procedures. At the end of your project work, you should have procedures defined that deal with incident response, policy management, disaster response and compliance for day-to-day operations. Once project work is completed, you should have updated policies and procedures for daily operations.

Project Work Breakdown Structure

Creating a work breakdown structure begins with your top level objectives. If you haven't defined those top level objectives yet, you can do so now. Ideally, you should define three to five top level objectives, though in some cases you might reasonably come up with six or seven. Too many and you've gone into too much detail too early, too few and you may be overlooking something or may not fully understand your project. Since we've been working with four project elements, let's use those as our four objectives. If your project is not going to cover these four areas, you can modify your project's WBS as needed.

1. Develop Incident Response Plan

    1.1 Assess incident response risk

    1.2 Develop incident response plan

        1.2.1 Develop network incident response plans

        1.2.2 Develop communication incident response plans

        1.2.3 Develop Web incident response plans

        1.2.4 Develop perimeter incident response plans

        1.2.5 Develop server and host incident response plans

        1.2.6 Develop infrastructure component (wireless, routers, DHCP, etc.) incident response plans

    1.3 Develop incident response team

        1.3.1 Develop incident response skills requirements

        1.3.2 Develop incident response operational procedures and processes

        1.3.3 Define incident response legal and regulatory requirements

        1.3.4 Define incident response documentation requirements

1.3.5 Define incident response reporting and escalation requirements

1.4 Develop incident response notification plan

1.4.1 Define notification process for local management

1.4.2 Define notification process for corporate IT management

1.4.3 Define notification process for regional or global management

1.4.4 Define notification process for local law enforcement action

1.4.5 Define notification process for national law enforcement (FBI, Homeland Security) action

1.5 Develop plan testing methodology

1.6 Develop plan test schedule

1.7 Develop plan maintenance schedule

1.8 Develop on-going team training processes

2. Develop Policy Management System

2.1 Review current policies

2.1.1 Review current policy management practices

2.1.2 Develop procedures for categorizing and assessing security policies

2.1.3 Develop policy management assessment and summary

2.2 Develop list of current policies

2.2.1 Inventory all applicable policies

2.2.1.1 Name of policy

2.2.1.2 Date of policy

2.2.1.3 Category or topic of policy

2.2.1.4 Scope of policy

2.2.1.5 Exclusions to policy

2.2.1.6 Owner of policy

2.2.2 Organize policies by category

2.3 Identify policy gaps

2.3.1 Identify gaps in policy by topic area

2.3.2 Identify gaps in policy by last update (i.e. a policy written in 1997 is more at risk than a policy written in 2005).

2.3.3 Identify gaps in policy by business area

2.3.4 Identify gaps in policy based on compliance areas

2.3.5 Develop gap analysis summary and action plan

2.4 Develop, revise and update policies based on Task 2.3.5

2.5 Conduct policy review prior to release

2.6 Release updated policies

2.7 Develop policy management/maintenance plans

3. Disaster Planning

3.1 Examine and analyze potential threats and vulnerabilities

3.1.1 Assess facilities vulnerabilities

3.1.2 Assess hardware and software vulnerabilities

3.1.3 Assess communications vulnerabilities

3.1.4 Assess data files vulnerabilities (confidentiality, integrity, availability)

3.1.5 Assess customer services vulnerabilities

3.1.6 Assess user operations vulnerabilities

3.1.7 Assess IT network and communication services (remote access, email) vulnerabilities

3.1.8 Assess end-user systems vulnerabilities

3.1.9 Assess other processing operations vulnerabilities

3.2 Assess impact of a disruption to normal services

3.2.1 Identify alternative business process handling

3.2.2 Identify customer service backup and recovery

3.2.3 Administration, operations, communications and IT

3.2.4 Identify compliance issues related to disaster management

3.3 Prepare information about existing systems

3.4 Review involvement of emergency services

3.5 Prepare initial assessment of potential impact of emergency

3.6 Define processes and procedures for mobilizing the recovery teams

3.7 Define processes and procedures for notifying employees, families and the media

3.8 Define processes and procedures for maintaining suitable records and event logs

4. Regulatory Compliance

4.1 Identify regulations that apply to organization

4.2 Identify specific compliance requirements

4.2.1 Identify required administrative procedures

4.2.2 Identify required physical safeguards

4.2.3 Identify technical security services required

4.2.4 Identify technical security mechanisms required

4.2. Identify policies and procedures required to gain compliance

4.3 Implement changes required for compliance

4.4 Identify policies and procedures required to maintain compliance

4.5 Implement policies and procedures required to maintain compliance

4.6 Identify procedures for reporting non-compliance

4.6.1 Identify procedures for reporting non-compliance to company management

4.6.2 Identify procedures for reporting non-compliance to regulatory bodies

4.6.3 Identify procedures for emergency response to non-compliance

4.6.4 Identify procedures for non-emergency response to non-compliance

4.7 Identify legal requirements for reporting and documentation

4.8 Identify requirements for on-going compliance audits

4.9 Identify requirements for on-going compliance maintenance activities

Remember to check your scope against your functional, technical and regulatory requirements and make sure everything syncs up. This is one place that scope begins to creep out of control and ensuring that your requirements are reflected in your WBS and that the WBS reflects your requirements is a great checkpoint in your project planning process. Also, if anything has changed (or even if it hasn't), this is also a good time to sit down with your project sponsor and review the project before project work begins. If any changes need to occur, now's the time to make them.

Task details are developed after your WBS. Remember the basics. Tasks should have one and only one owner, though others may contribute to task work. Task details help drive quality, so be sure to have subject matter experts assist in developing task details, especially completion criteria. Note any dependencies, constraints or requirements associated with tasks so you can build them into your project schedule and budget. Identify how long a task will take (duration allotted) and how much you expect it to cost. Some projects work with hard costs only and do not track direct project labor. Other companies want people to keep timesheets to track time against specific projects. This is especially true in consulting firms, but your firm may also require this level of tracking.

Project Risks and Mitigation Strategies

The risks to an operational security plan are as varied as the tasks within the plan. Let's break it down based on the four high level objectives and we can walk through a few of the possible risks. You and your project team should sit down, identify the risks and rank them based on their likelihood of occurring and the criticality of such an occurrence. Then, you can choose how far down the prioritized list to go in your planning session. For each risk, develop a mitigation strategy that includes potential ways to avoid the risk altogether or ways to reduce the impact of the risk should it end up occurring. Finally, be sure to include triggers so you know when you'll implement your mitigation plan. If appropriate, you should also look at potential risks your alternative strategies may inject into your project plan. In some cases, you may find that you'd rather deal with a particular risk, should it occur, than to implement a more flawed "Plan B."

Incident response

Remember, risk planning is not the risk that an incident will occur but the risk that something will impact our incident response project plan. What are the things that could put that project segment at risk? Things like a corporate re-organization, acquisition or spin-off certainly would impact your project. Staff layoffs could decimate your response team; budget cutbacks could impact your team's ability to remain current on threats and vulnerabilities. Budget cutbacks could also put equipment (hardware, software) purchases at risk. Changes in the legal or compliance markets could imperil your incident response project plan as well.

Policy management

Changes in the management structure or philosophy of the company could certainly put a policy management project at risk. Another potential risk to this part of the project is the other corporate-wide disruptions including re-organizations, acquisitions, spin-offs that would impact the scope of the project. Layoffs could impact your ability to complete the project. Changes in the legal or regulatory environment could certainly put a project of this nature at risk. The project could also be delayed by changes in technology, so the project should be coordinated with any major infrastructure changes such as the implementation of a wireless network, the upgrading of remote access technologies or the introduction of new authentication technologies, to name a few.

Disaster planning

You disaster planning is also subject to the same macro-level considerations as the previous two topics covered. Changes to various infrastructure components such as the introduction of a new facility or the closing of an older one that was providing data services or backup functions could impact your disaster planning project. You and your team should look closely at what could impact your disaster planning and address these because when it's all said and done, you need a solid disaster recovery plan in place. You need to test that plan and keep it up-to-date so that if a disaster strikes, you have some reasonable path to follow. Budget cuts, layoffs and other organizational change can dramatically impact your disaster readiness, so you should give this area of risk mitigation serious attention.

Regulatory/compliance

The biggest risks to this section of your project plan involve things generally outside of your control whether that's changes to the language or intent of the regulations or lack of clarity about requirements for compliance. This is an area where you should involve executives and legal counsel, if appropriate, to ensure you've covered the potential risks and understand the intricacies of this environment.

Project Constraints and Assumptions

Utilize this section of your project plan to list any known constraints to your project as well as any assumptions under which you're operating. Constraints are usually restrictions impacting your project as a whole such as resource limitations or constraints imposed by other corporate initiatives or directives. Constraints could also come from the legal or regulatory environment, so be sure to look at these as well.

Assumptions are critical to include in your project plan because with every project, we make certain assumptions about the environment that will be in place when we commence project work. Examples of assumptions include staffing levels, expertise on your IT project team or the timing of other key events. While it's sometimes hard to see exactly what we're assuming to be true about a situation, work with your project team to identify these assumptions and document them in your project plan. Run them by your project sponsor to be sure they're acceptable assumptions. If you assume that the company will proceed with purchasing and implementing an IDS or IPS system and it doesn't, your incident response plan could change significantly. If you're assuming your company will remain at its current size and number of locations, list that since any change could impact all areas of your operational security plan.

Project Schedule and Budget

At this point, you should have all the data you need to develop a preliminary schedule and budget based on the information defined in your WBS. You'll need to enter your WBS into a project management software tool if you want to use automated scheduling features (highly recommended). You'll need to look at resource constraints as well as dependencies. In this project, you may have four sub-teams performing project work but there may be overlap. It's conceivable (perhaps likely) that you'll have the same or overlapping resources on your policy management section and on your compliance section because these two areas are so closely connected. You may also have the same or an overlapping group of people working on your incident response section and your disaster planning section. Be sure you account for overlapping resource conflicts in your schedule. You also need to identify dependencies for the project. These will probably have common characteristics the four sections. For example, your policy group's timing will depend on the timelines of the incident response team, the disaster recovery team and the compliance team because policies cross all those boundaries. Look for these areas and be sure that your schedule accommodates these. Once you've loaded in your dependencies, check your critical path. If all (or none) of your tasks are on the critical path, something's wrong and you'll need to go back through your schedule to see what's going on.

Each task contains details regarding cost, so you should also be able create a realistic budget for your project at this point. Both schedule and budget should be reviewed with your project sponsor and signed off on. If there are any problems, resolve them now before project work begins.

One final note on project budgets – you will need to have on-going activities to support network security. Your project plan should include an assessment of the on-going activities and costs the company will incur to maintain security. This is typically less than the cost of going through another full-blown security assessment. Including information about the cost of on-going security operations at the end of your project, as part of project close-out can help you budget moving forward.

IT Operational Security Project Outline

1. Develop Incident Response Plan
    - 1.1 Assess incident response risk
    - 1.2 Develop incident response plan
    - 1.3 Develop incident response team
    - 1.4 Develop incident response notification plan

- 1.5 Develop plan testing methodology
- 1.6 Develop plan test schedule
- 1.7 Develop plan maintenance schedule
- 1.8 Develop on-going team training processes

2. Develop Policy Management System
    - 2.1 Review current policies
    - 2.2 Develop list of current policies
    - 2.3 Identify policy gap
    - 2.4 Develop, revise and update policies based on Task 2.3.5
    - 2.5 Conduct policy review prior to release
    - 2.6 Release updated policies
    - 2.7 Develop policy management/maintenance plans
3. Disaster Planning
    - 3.1 Examine and analyze potential threats and vulnerabilities
    - 3.2 Assess impact of a disruption to normal services
    - 3.3 Prepare information about existing systems
    - 3.4 Review involvement of emergency services
    - 3.5 Prepare initial assessment of potential impact of emergency
    - 3.6 Define processes and procedures for mobilizing the recovery teams
    - 3.7 Define processes and procedures for notifying employees, families and the media
    - 3.8 Define processes and procedures for maintaining suitable records and event logs
4. Regulatory Compliance
    - 4.1 Identify regulations that apply to organization
    - 4.2. Identify policies and procedures required to gain compliance

4.3 Implement changes required for compliance

4.4 Identify policies and procedures required to maintain compliance

4.5 Implement policies and procedures required to maintain compliance

4.6 Identify procedures for reporting non-compliance

4.7 Identify legal requirements for reporting and documentation

4.8 Identify requirements for on-going compliance audits

4.9 Identify requirements for on-going compliance maintenance activities

Summary

You can secure your network using hardware and software but if you don't develop operational plans to maintain that security, you still have significant risk to your network. Operational security involves developing incident response teams that can address three major areas of security: security management, proactive services and reactive services. Your response team planning project (or sub-project) should address these areas and provide on-going support for network security. The work of the response team overlaps other areas of the organization and including key stakeholders in the response team's planning and implementation will help provide a more comprehensive approach to incident management.

Policies and procedures are vital to on-going security operations. The IT staff will need updated policies and procedures for managing day-to-day security and users will need updated policies and procedures to help them do their part to maintain a safe and secure network environment. Most companies have policies and procedures related to network and computer security but they are often implemented in a haphazard or lax manner, resulting in security lapses. Since a large number of internal security breaches are the result of someone intentionally or unintentionally disregarding security policies, this is an area that will bolster network security significantly. Review and revise policies then make sure they're kept up-to-date and that users are well aware of them. Using targeted education and awareness campaigns, you can be sure your users have the tools they need to help maintain a secure computing environment.

Disaster planning is the subject of entire books, so we only covered the basics in this chapter. However, you should be aware that disaster planning and recovery are part of the larger business continuity planning function. As such, your project team should include stakeholders from every corner of the organization. In some companies, the IT staff heads up BC planning because so much of the work involves ensuring network services become quickly available after a disaster. In other companies, IT staff participates as part of a corporate project team to perform overall BC planning that incorporates IT plans.

Regulations regarding confidentiality and privacy have proliferated in recent years and almost every IT staff has to deal with some sort of regulations. While this can be an onerous task, working within a consistent methodology such as IT project management can make the task more manageable. Failure to comply with regulations can be costly in some cases; in other cases, it can be the cause of serious legal action. To avoid these problems, be sure to understand your company's compliance issues and seek expert advice as you move toward compliance. Some regulatory agencies have provided very clear guidelines; other guidelines are vague or contradictory. Addressing these issues within an IT project management framework can help you support and defend your position and ultimately get you close to achieving and maintaining compliance.

All four of these areas have overlapping segments and taking an integrated approach to operational security will help you avoid gaps that can be created by looking at these areas as individual projects. Operational security project plans are often developed and implemented in parallel or subsequent to other IT security project plans because they provide the framework for maintaining IT security once achieved. This critical step should be undertaken with the same attention to security and detail as every other IT security project plan and should be the final piece of the puzzle in maintaining a secure environment. Network and IT security is a never-ending job, but putting solid operational plans in place will help reduce the burden by building in practices and procedures that support and enhance IT security.

Solutions Fast Track

Operational Security Assessment

☑ Operational security planning and implementation helps support and enhance network security through addressing the on-going security needs of the organization.

☑ These on-going needs can be broken down into five main areas: Incident response, security policies, disaster recovery, regulatory compliance and configuration management

☑ Incident response is typically managed through the creation of a response team.

☑ The response team's mission can be broken down into three areas: security management services, proactive services and reactive services. Together, these three areas address the on-going security services needed to maintain a secure network environment.

☑ Most companies have policies related to network security including IT operational procedures or policies and user policies.

☑ Policies that are not current are a liability to network security because they may require or advise users to take actions that are no longer appropriate or that cause confusion.

☑ Policies should be written in a clear, concise and easy-to-understand manner that enables the intended audience to quickly and easily understand what is required to maintain security.

☑ Awareness campaigns are an important part of promulgating security policies. Raising user awareness about security issues, especially in an environment where security threats change everyday, can mean the difference between an attempted intrusion and a successful one.

☑ Disaster planning is part of the larger business continuity planning process.

☑ Disaster planning is often part of the mission of the response team and there may be overlap in these planning processes.

☑ Disaster planning should include facilities, operations, IT operations and business functions.

☑ The regulatory environment is constantly changing and you may need outside expertise or legal counsel to assist in your compliance planning.

☑ Using a project management methodology will help in gaining and maintaining compliance.

☑ Be sure to build compliance requirements into your project plan so that you can use your project plan as a means toward compliance.

Project Parameters

☑ Executive support is essential to the success of all projects, but even more so to IT operational projects that span the organization.

☑ Define your functional and technical requirements with an eye toward compliance issues to reduce your challenges in this area.

Project Team

☑ Be sure to create a cross-functional team for your operational security. There are often issues outside of the IT department that should be taken into consideration during the planning phase.

☑ An operational security project requires slightly different skills than a purely technical project. These included the ability to perform organizational audits, to develop policies and procedures and to create consistent, clear and useable documentation.

Project Organization

☑ An operational security plan requires a bit more cross-departmental coordination due to the wide reaching nature of operations.

☑ Some operational security planning can be done in parallel with other project work; other planning must be done only at the conclusion of other project work. Identify areas where working in parallel is feasible (and desirable) to avoid working at cross-purposes.

Project Work Breakdown Structure

☑ Your Work Breakdown Structure development should begin with developing the high level objectives of the project.

☑ The four high level objectives for your operational security project plan include incident response, policy management, disaster planning and regulatory compliance.

☑ Task details should be developed by subject matter experts.

☑ Task details should include compliance or regulatory requirements so that when project work is complete, the bulk of the compliance work has been completed as well.

Project Risks and Mitigation Strategies

☑ Every project has risks that must be addressed. When working on an operational security project plan, your risks are often related to the wider organizational environment.

☑ In some cases, mitigating your risks can cause more operational problems than the risk itself. After identifying operational security risks, determine whether your "Plan B" introduces more risk than the original action.

Project Constraints and Assumptions

☑ Constraints limit your ability to complete project work. Constraints are external to the project itself and have to do with the organizational environment in which the project is being managed.

☑ Listing assumptions is critical for project success because if any of the elements you're assuming to be true or present changes, your entire project is at risk.

☑ In an operational security project plan, constraints and assumptions can be related to corporate-wide actions such as acquisitions, divestitures, joint ventures and other business relationships.

☑ Operational security plans are also impacted by impending hiring or layoff plans. Disruptions to your corporate-wide operational security project team can derail even the best project plans.

Project Schedule and Budget

☑ The schedule for your operational security project plan requires coordination across a variety of functional areas.

☑ Some operational security components can be done in parallel with other activities. In some cases, the operational security planning must be done only at the completion of other project (typically more technical projects) so that security can be maintained on a going-forward basis.

☑ The budget for an operational security budget often is more heavily weighted toward labor costs than expenditures for tools, technology or equipment.

☑ Be sure your project budget can later be translated into a budget to support on-going security operations.