Chapter 9

Corporate IT Security Project Plan

Solutions in this chapter:

- Defining Your Security Strategy
- Legal Standards Relevant to Corporate IT Security
- Corporate IT Security Project Plan Overview
- Corporate Security Auditing
- Corporate Security Project Parameters
- Project Work Breakdown Structure
- Project Risks
- Project Constraints
- Project Assumptions
- Project Schedule and Budget

Warning: Do Not Practice Law Without a License

In virtually every U.S. state, individuals are legally prohibited from practicing law without a license. For example, in Colorado, "practicing law" is defined, by law, to include, "counseling, advising and assisting [another] in connection with" legal rights and duties. Penalties for the unauthorized practice of law in Colorado can include fines or imprisonment. Information security consultants should not, under any circumstances, purport to advise customers as to the legal implications of statutes such as the HIPAA, Gramm-Leach-Bliley financial information privacy provisions, or other federal, state, or local laws or regulations. First, the consultants risk legal action against them by doing so. Second, they do their customers a grave disservice by leading them to believe that the customers can take any legal comfort from advice given them by non-lawyers.

Introduction

This chapter provides the framework for creating an overarching corporate Information Technology (IT) security project plan. In subsequent chapters, we'll step through Individual Security Area Projects (ISAPs). This and subsequent chapters are intended to be used as templates to guide you through your security project planning process. There is no one-size-fits-all approach to any security project planning process; thus, you will need to modify your security project plan to fit your organization's requirements. This chapter provides the basic building blocks to help you get started. As you read this chapter, keep in mind that the same principles apply, with some variation, to each of the ISAPs discussed later in this book. As you become familiar with the framework used in this chapter, you'll be able to see more clearly how this and subsequent ISAP plans should be modified to fit your own unique needs. This chapter also discusses a security audit.

Defining Your Security Strategy

Managing IT security across an enterprise is one of the most important business problems you'll face in your IT career. IT security impacts the ongoing viability and competitiveness of your company. Regardless of the assets and resources that need to be secured (information, technology, assets), you must have a clear strategy you can implement, monitor, and revise as the business and operational environments change. In the long run, the effectiveness of your overall IT security strategy depends on how well it is aligned with and supports the organization's business drivers. Your corporate IT security project plan must provide the strategic vision for how you address enterprise-wide IT security. Many organizations understand that IT security project success depends on gaining executive-level management support and aligning security goals with the mission, vision, and objectives of the organization. When IT security is aligned with business objectives, security becomes a tool to enable and support your company's strategy, rather than just a black hole for IT expenditures.

Your corporate IT security project essentially defines your security strategy for the organization. While it must include specific deliverables related to key areas of enterprise security, it also needs to address the higher level strategic security approach. Clearly, your security strategy should be aligned with organizational objectives in order to add value to the organization and gain key management support. Your security strategy should be defined prior to initiating your corporate IT security planning process so that you have a clear view of the required objectives. Your corporate IT security plans also have to align with the reality of your organization. You must live within the company's constraints, which may include budget, schedule, staffing, or other overarching organizational limitations. It doesn't matter if you create a masterful security strategy or project plan if it costs far more than your company can afford or requires resources your company doesn't have. Your goal should be to find an optimal solution that fits within the constraints of the organization.

A technical report, written by Richard Caralli at Carnegie Mellon entitled "The Critical Success Factor Method: Establishing A Foundation For Enterprise Security Management" (Technical Report, CMU/SEI-2004-TR-010, ESC-TR-2004-010, July 2004), identifies the following five key success factors in developing an enterprise security strategy:

- The skills, capabilities, and efforts of the entire organization must be utilized and mobilized.
- The key functions and processes in the organization must collaborate on shared security goals and strategy.
- The organization's security objectives or an articulation of its "desired state" must be developed and understood.
- Critical assets that are essential to achieving the organization's mission must be identified and protected.
- IT operations and support must enable security goals.

It should be evident that if you lack a strategic view of security in the enterprise, you'll have difficulty getting executive support for your initiatives. As you learned in Chapter 1, executive support for IT projects is the number one success factor. Developing a security strategy that supports and enhances organizational goals is the primary way to achieve your IT security mission-critical objectives. With that in mind, we'll dig into developing a corporate IT security plan that supports your organization's objectives. In addition, your strategy should take into account the predominant legal issues your organization might have to contend with.

Legal Standards Relevant to Corporate IT Security

WARNING: THIS SECTION DOES NOT CONTAIN LEGAL ADVICE

This section provides an overview of a number of legal issues faced by information security professionals and their companies. Hopefully, it will alert you to the issues on which you should consult qualified legal counsel experienced in information security law. This chapter, however, does not, and cannot, provide any legal advice or counsel to you. **You should not, under any circumstances, purport to rely on anything in this book, chapter, or section "Legal Standards Relevant to Corporate IT Security," as legal advice**. Likewise, following any of the suggestions in this section does not create an "advice-of-counsel" defense to regulatory or law enforcement action or to civil legal claims. If you are involved in information security and have any questions regarding the law and IT security, you are strongly urged to retain qualified, experienced legal counsel.

The following sections discuss the legal standards relevant to IT security. The corporate IT security project plan is the appropriate place to discuss these elements, because you need to be cognizant of the legal issues surrounding IT as you formulate your comprehensive security project plan. As written in the above sidebar, nothing in this section (or book, for that matter) should be construed as legal advice in any manner. Instead, it is provided as an overview of some of the legal issues involved with IT security. Some IT professionals fail to understand the legal implications for IT security and put themselves and their companies at substantial legal risk. This section is intended to give you a jump start in understanding some of the issues so you can determine for yourself what additional resources and assistance you might need to ensure that you and your company are adequately protected.

We know that laws are made by politicians and that politicians are driven by public and media reaction to specific incidents. As is often the case, laws are made piecemeal to deal with individual incidents. At some point, a critical mass is reached and lawmakers may patch together a number of initiatives to address a growing concern. The result, however, is often a set of laws that are inconsistent, piecemeal, spotty, and sometimes contradictory.

This is the current situation in the law of information security. As discussed in "Selected Federal Laws" below, federal law regulates information security for, among other things, personally identifiable health care information, financial information of individuals, and, to an increasing degree, financial information in the hands of publicly traded companies. There currently is no "omnibus" federal statute governing all information security. Instead, the standards are pieced together in response to various perceived (and actual) problems found in the public and private sector.

For IT security professionals, this is a good news/bad news story. Often, attempts at "comprehensive" legislation turn out to be a jumbled mess, particularly when multiple economic sectors with differing operational environments and needs are being regulated, and lawmakers lack a clear understanding of the technological issues at hand. Such regulation can be particularly ineffective (or worse) when forced upon the private sector. On the other hand, a patchwork of different federal, state, and international laws and regulations (as is the current state of information security law) can be confusing and puts a premium on careful, case-specific legal analysis and advice from qualified and experienced counsel.

If you're reading this wondering how your small company can afford to address these legal issues, there is some good news. First, you can do your own research and become conversant with the various legal issues relevant to your company's IT security. First, you can do your own research and become conversant with the various legal issues relevant to your company's

IT security.You should be aware, however, that doing your own research provides you with no legal protection, unless you get a legal opinion from qualified outside legal counsel. At a minimum, you should take this information to a competent attorney that specializes in IT security and understands your business sector to get a legal opinion to protect your company's interests. If you do your homework, your legal bills will be far less than if you walk in the door unprepared. Have specific questions prepared and then ask "What else do I need to know?" It may not be your specific responsibility to do this, but as the IT security project manager for your company, you have the responsibility to bring these potential legal issues to the attention of senior management so they can make the determination as to the best way to address and mitigate legal risks.

Selected Federal Laws

To illustrate the array of laws that impact information security, the following provides a general survey of statutes, regulations, and other laws that may govern information security consultants and their customers. This list is not exhaustive, but may help identify issues and understand which "best practices" have actually been adopted in law. If any of these areas apply to your company, you can do additional research, consult your in-house counsel, or hire outside counsel to advise you on how to ensure your company's legal exposure is reduced to the greatest degree possible.

Gramm-Leach-Bliley Act

One of the earliest US government forays into mandating information security standards was the Gramm-Leach-Bliley Act (GLBA). Section 501(b) requires each covered financial institution to establish "appropriate safeguards" to: (1) ensure the security and confidentiality of customer records and information; (2) protect against anticipated threats or hazards to the security or integrity of those records; and (3) protect against unauthorized access to, or use of, such records or information which could result in substantial harm or inconvenience to any customer. GLBA required standards to be set by regulation for safeguarding customer information. This task was accomplished with the publishing of the

Interagency Guidelines Establishing Standards for Safeguarding Customer Information (the "Guidelines"). The Guidelines apply to customer information maintained by covered "financial institutions," both of which terms are broadly defined under applicable law and regulations. The Guidelines require a written security program specifically tailored to the size and complexity of each individual covered financial institution, and to the nature and scope of its activities. Under the Guidelines, covered institutions must conduct risk assessments to customer information and implement policies, procedures, training, and testing appropriate to manage reasonably foreseeable internal and external threats. Institutions must also ensure that their Board of Directors (or a committee thereof) oversees the institution's information security measures.

Further, institutions must exercise due diligence in selecting and overseeing, on an ongoing basis, service providers (entities that maintain, process, or otherwise are permitted access to customer information through providing services to a covered institution). Institutions also must ensure, by written agreement, that service providers maintain appropriate security measures.

Health Insurance Portability and Accountability Act

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) became law in August 1996. Section 1173(d) of HIPAA required the Secretary of Health and Human Services (HHS) to adopt security standards for protection of all Electronic Protected Health Information (EPHI). Development of these security standards was left to the HHS Secretary, who released the HIPAA Security Final Rule (the "Security Rule") in February 2003. All covered entities, with the exception of small health plans, must now comply with the Security Rule. Because HIPAA has, in some ways, the most elaborate and detailed guidance available in the realm of federal law and regulation with regard to information security, we focus more on the HIPAA Security Rule than any other single federal legal provision. In addition, many of the general principles articulated in the Security Rule are common to other legal procedures dealing with information security. In general, the HIPAA

Security Rule mandates specific outcomes and specifies process and procedural requirements, rather than specifically mandated technical standards. The mandated outcomes for covered entities are:

- Ensuring the confidentiality, integrity, and availability of EPHI created, received, maintained, or transmitted by a covered entity
- Protecting against reasonably anticipated threats or hazards to the security or integrity of such information
- Protecting against reasonably anticipated uses or disclosures of EPHI not permitted by the HIPAA Privacy Rule
- Ensuring compliance with the Security Rule by its employees.

Beyond these general, mandated outcomes, the Security Rule contains process and procedural requirements broken into several general categories:

- **Administrative Safeguards** Key required processes in this area include: conducting a comprehensive analysis of reasonably anticipated risks; matrixing identified risks against a covered entity's unique mix of information requiring safeguarding; employee training, awareness, testing, and sanctions; individual accountability for information security; access authorization, management, and monitoring controls; contingency and disaster recovery planning; and ongoing technical and non-technical evaluation of Security Rule compliance.
- **Physical Safeguards** Physical security safeguard measures include: mandated facilities access controls; workstation use and workstation security requirements; device and media controls; restricting access to sensitive information; and maintaining offsite computer backups.
- **Technical Safeguards** Without specifying technological mechanisms, the HIPAA Security Rule mandates automated technical processes intended to protect information and to control and record access to such information. Mandated processes include authentication controls for persons accessing EPHI, encryption/

decryption requirements, audit controls, and mechanisms for ensuring data integrity.

The Security Rule contains other requirements beyond these general categories, including: ensuring by written agreement that entities with whom a covered entity exchanges EPHI maintain reasonable and appropriate security measures, and holding those entities to the agreed-upon standards; developing written procedures and policies to implement the Security Rule's requirements, disseminating such procedures, and reviewing and updating them periodically in response to changing threats, vulnerabilities, and operational circumstances.

Sarbanes-Oxley Act

The Sarbanes-Oxley Act of 2002 (SOX) has gotten a lot of media attention in the past few years and came on the heels of some very well-publicized corporate scandals, most notably the collapse of Enron. SOX creates legal liability for senior executives of publicly traded companies, potentially including stiff prison sentences and fines of up to $5,000,000 per violation, for willfully certifying financial statements that do not meet the requirements of the statute. Section 404 of SOX requires senior management, pursuant to rules issued by the Securities and Exchange Commission (SEC), to attest to: "(1) the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting; and (2) …the effectiveness of the internal control structure and procedures of the issuer for financial reporting." (See Chapter 13 sidebar "SEC Announces Next Steps for Sarbanes-Oxley Implementation to Help Small Companies" for an update on recent changes related to Section 404). Section 302 also requires that pursuant to SEC regulations, officers signing company financial reports certify that they are "responsible for establishing and maintaining internal controls," and "have evaluated the effectiveness" of those controls and reported their conclusions as to the same.

Federal Information Security and Management Act

The Federal Information Security and Management Act of 2002, as amended, (FISMA) does not directly create liability for private sector IT security professionals or their companies. However, IT security professionals should be aware of this law, because it:

- Legally mandates the process by which information security requirements for federal government departments and agencies must be developed and implemented
- Directs the federal government to look to the private sector for applicable "best practices" and to provide assistance to the private sector (if requested) with regard to information security
- Contributes to the developing "standard of care" for information security by mandating a number of specific procedures and policies

If you work for the federal government or an organization that comes under federal auspices, your organization may be directly impacted by FISMA.

FERPA and the TEACH Act

The Family Educational Right to Privacy Act (FERPA) prohibits educational agencies and programs, at risk of losing federal funds, from having a policy or practice of "permitting the release of " specified educational records. FERPA does not state whether or not the prohibition places affirmative requirements on educational institutions to protect against unauthorized access to these records through the use of information security measures. It is certainly possible that a court could conclude in the future that an educational institution which fails to take reasonable information security measures to prevent unauthorized access to protected information is liable under FERPA for "permitting the release" of such information. The recent case of a Vermont college system employee having such data on a laptop that was later stolen (see Chapter 1 sidebar "The Real Cost of Remediation") might test this very statute. The 2002 Technology, Education, and Copyright Harmonization Act (the "TEACH Act") explicitly requires educational institutions to take "technologically feasible" measures to prevent unauthorized sharing of copyrighted information beyond the students specifically requiring the information for their studies, and, thus, may create newly enforceable legal duties on educational institutions with regard to information security.

Electronic Communications Privacy Act and Computer Fraud and Abuse Act

These two federal statutes, while not mandating information security procedures, create serious criminal penalties for any persons who gain unauthorized access to electronic records. Unlike laws such as HIPAA and GLBA, these two statues broadly apply, regardless of the type of electronic records that are involved. The Electronic Communications Privacy Act (ECPA) makes it a federal felony to use or intercept the contents of electronic communications without authorization. In addition, the Computer Fraud and Abuse Act of 1984 (CFAA) makes it a felony to gain unauthorized access to a very wide range of computer systems (including financial institutions, the federal government, and any protected computer system used in interstate commerce). As a result, IT security professionals, especially outside consultants who may test client security (i.e., try to hack into a system to gain unauthorized access) must take great care, and rely on qualified and experienced legal professionals to ensure they receive authorizations from their clients that are broad and specific enough to mitigate potential criminal liability under the ECPA and the CFAA.

Business Intelligence…

What to Look For in Your Attorneys

There are a number of obvious characteristics one should seek in any attorney retained for any purpose. These include integrity, a good repu-

Continued

tation in the legal community, and general competence. You also want to consider an attorney with a strong background in corporate and business transactions who is familiar with the contracting process. One useful tool for evaluating these qualities as you attempt to narrow your list of potential attorneys to interview is a company called Martindale Hubbell (www.martindale.com). Look for lawyers with an "AV" rating (Martindale's highest).

(Note: Never hire any attorney without at least one face-to-face meeting to learn what your gut tells you about whether you could work with him or her.)

In the area of information security evaluation, you will want to look for attorneys with deep and broad expertise in the field. The best way to do so is to look for external, independently verifiable criteria demonstrating an attorney or law firm's tested credentials (e.g., is the lawyer you seek to retain listed on the National Security Agency Web site as including individuals certified as having been trained in NSA's Information Security Assurance Methodology (IAM)? If so, on the appropriate NSA Web page (e.g., www.iatrp.com/indivu2.cfm#C), you will find a listing similar to this: Cunningham, Bryan, 03/15/05, (303) 743-0003, bc@morgancunningham.net)

Has an attorney you are considering authored any published works in the area of information security law? Has he or she held positions, in the government or elsewhere, related to information security? Finally, there's the gut check. How does your potential lawyer make you feel? Are you comfortable working with him or her? Does he or she communicate clearly and concisely? Does he or she seem more interested in covering their own backside than in providing you with legal counsel to protect your interests?

State Laws

In addition to federal statutes and regulations implicating information security, there are numerous state laws that, depending on an entity's location and the places in which it does business (also known as *nexus*), can also create legal requirements related to the work of information security professionals.

Unauthorized Access

In Colorado (and in other states), it is a crime to access, use, or exceed authorized access to, or use of, a computer, computer network, or any part of a computer system. It is a crime to take action against a computer system to cause damage, to commit a theft, or for other nefarious purposes. However, it is particularly important for IT security professionals to be aware that it is also a crime to knowingly access a computer system without authorization or to exceed authorized access. This is one reason it is critical for IT security consultants, with the advice of qualified and experienced counsel, to negotiate a comprehensive, carefully worded, Letter of Authorization (LOA) with every client.

If you are hiring an outside consultant, they should insist on this type of authorization if they plan on testing your network's security. If they do not insist on this (or even mention it), you should seriously review the consultant's credentials to be sure they have the requisite skills and knowledge you're looking for. If they are not hired to actually test your system for vulnerabilities and will not be testing for the ability to gain unauthorized access, this type of LOA may not be needed. On the other hand, if a consultant asks for this type of authorization and it's not what you hired them to do, it should signal a serious disconnect that should be addressed before going any further. Be sure you're hiring a bona fide consultant and not a rogue hacker in a business suit.

Enforcement Actions

What constitutes the "reasonable standard of care" in IT security will continue to evolve, and not only through new statutes and regulations. Prosecutors and regulators will not be content to wait for such formal, legal developments. In lawsuits, prosecutors and regulators have demonstrated the clear intent to extend "reasonable" IT security measures even to those entities not clearly covered by specific existing laws. This is being done through legal actions leading to settlements, often including consent decrees (agreements entered into to end litigation or regulatory action) wherein a company agrees to "voluntarily" allow regulators to monitor (e.g., for 20 years) the company's IT security program. Such was the case with the company that ended up purchasing CardSystems, the credit card transaction processing company that was responsible for millions of credit card holders' information being compromised (described in Chapter 1).

Since these agreements are publicly available, they are adding to the "standard of care" to which organizations will be held. They also provide added support for similar enforcement actions in the future. Thus, even if your company is not specifically required by law to take certain security measures, it might still suffer rigorous legal consequences for its actions.

Three Fatal Fallacies

The saying goes, "A little knowledge is a dangerous thing." The same can be said of conventional wisdom. Unfortunately, many organizations and IT professionals, upon realizing they have legal and other requirements for IT security, have come to believe incorrect information regarding their security decisions. Let's take a look at a few of these common misunderstandings.

The "Single Law" Fallacy

Many IT security professionals, both within companies and those working as consultants, subscribe to the "single law" fallacy. That is, once they identify the laws, statutes, or set of regulations they think apply to them, they address just those issues under the belief they've got their legal bases covered. In fact, this may or may not be the case. Rather than blithely making these assumptions, you or your company should seek competent legal advice to mitigate the legal risks. Take, for example, a mid-sized college or university. IT security professionals may conclude that, since FERPA clearly applies to educational records, following guidance tailored to colleges and universities based on what they conclude are the appropriate Department of Education standards, is sufficient to mitigate any potential legal liability. This could be an expensive assumption to make, particularly if the educational institution does not ask itself the following questions:

- Does the school grant financial aid or extend other forms of credit? If so, it could be subject to GLBA.
- Does it operate hospitals, provide psychiatric counseling services, or run a student health service? If so, it could be subject to HIPAA.
- Does the school's Web site contain any representations about the security of the site and/or university-held information? If so, it could be subject to lawsuits under one or more (depending on whether it has campuses in multiple states) state deceptive trade practices laws.

The Private Entity Fallacy

Focusing on SOX and the resulting preoccupation with publicly traded companies, some institutions take solace in being private and in the fact that, so the argument goes, they are not subject to SOX and/or that they can somehow "fly under the radar" of federal regulators. Anyone who believes that lawyers for future plaintiffs (students, faculty, victims of attack, or identity theft) will be deterred by the literal terms of SOX is misguided. The argument will be that the appropriate "standard of care" for IT security was publicly available and well known. And, just because your company may not specifically be obligated under SOX, there are numerous other segments of the law that could apply such as HIPAA, GLBA, state statutes, and common law theories and, depending on where an entity does business, international and foreign law, such as the complex and burdensome European Union Privacy Directive.

The "Penetration Test Only" Fallacy

Some IT security professionals are so confident in their security solutions and implementations that they hire an outside security consultant just to try to break into the system. This can be the case when the company is strapped for funds and doesn't believe it can afford an outside security consultant, or when the organization has a fairly strong group of IT professionals in-house. The problem is, if you hire an outside consultant to do a penetration test (also called a "pen test"), you are exposing your company to potential legal liabilities. Think of it this way. An IT security consultant performs a penetration test and gets in. He or she exposes one or more weaknesses in your system. This exposes vulnerabilities that are now publicly (or at least with an outside entity) documented and open to the legal discovery process. While you may hire an outside firm to do a penetration test at some point, it should be as part of a holistic approach to IT security utilizing both internal and if desired, external, resources.

Do It Right or Bet the Company: Tools to Mitigate Legal Liability

In recent years, numerous articles have been written on how to protect your network from a technical perspective, but, at least throughout mid-2005, the headlines were full of examples of companies that have lost critical information due to inadequate security. ChoicePoint, DSW Shoes, several universities, financial institutions including Bank of America and Wachovia, MasterCard and other credit providers, and even the FBI have been named in recent news articles for having lost critical information. As one example, ChoicePoint was sued in 2005 in actions brought in states ranging from California to New York and in its home state of Georgia. Allegations in the lawsuits included that ChoicePoint failed to "secure and maintain confidential the personal, financial and other information entrusted to ChoicePoint by consumers"; failed to maintain adequate procedures to avoid disclosing some private credit and financial information to unauthorized third parties; and acted "willfully, recklessly, and/or in conscious disregard" of its customers rights to privacy.

It's not hard to imagine that if you work for a medium-to-large company that deals with consumer data of any kind, that one day you may be faced with an IT security-related lawsuit, frivolous or not. The question is, what can you as the IT security project manager do to help your company reduce its litigation "target profile?" Creating a thorough corporate IT security project plan helps, but there are a few additional tips we've provided below.

We Did our Best; What's the Problem?

Many companies feel that their internal IT technology and security staffs are putting forth their best efforts to maintain and secure their networks. They may know there have been no significant security breaches and that the organization has well-defined procedures for handling important data. They may even hire an outside security consultant for periodic penetration tests that result in no penetration occurring. All's well, right? Not really. Simply doing one's best is not enough in today's litigious environment. Corporate efforts must also be grounded in complying with existing, external legal standards. In ChoicePoint's case, at least based on what has been made public, penetration tests would not have helped. ChoicePoint appears to have fallen victim to individuals who fraudulently posed as businessmen and conned people into giving them what may have been otherwise secure information. This was a classic case of social engineering at its best. Penetration testing would have shown that the networks were secure, but as we know, no network is completely secure and social engineering is a good example of that.

Addressing any one particular potential point of failure will almost never be enough. Companies today must understand the potential sources of liability that apply to all companies, as well as those specific to their industry. Companies can minimize their risk through understanding the legal environment and adopting and implementing policies to assure a high level of compliance with current legal requirements. Of course, this approach cannot be non-static, either. It requires an ongoing review and implementation to assure compliance in an ever-changing legal environment. As part of your corporate IT security plan, you should be sure that your project plan includes the ongoing security maintenance and monitoring activities needed to continually assess and improve your organization's security measures. (This topic is addressed in more detail in Chapter 13.)

Negligence and the "Standard of Care"

Clearly, there are numerous variations to the ways IT security can be breached and how those breaches can impact companies and individuals (customers, employees, and so forth). Understanding the basis for liability and conducting business in a manner designed to avoid liability is the best defense. In many cases, the claim of liability is based on a charge that the company and its officers and directors acted "negligently." In law, "negligence" arises when a party owes a legal duty to another, that duty is breached, and the breach causes damages to the injured party. Generally speaking, acting "reasonably" under the circumstances will prevent companies from being found "negligent." The problem is that the definition of "reasonable" can be tricky and changeable.

When a company maintains personal or confidential customer information, or has agreed to maintain as confidential the trade secret information of another business, its minimum duty is to use reasonable care in securing its computer systems to avoid theft or inadvertent disclosure of the information entrusted to it. Reasonable care may be an extremely high standard when trust and confidence are placed in a company to secure sensitive information. A reasonable "standard of care" is what the law defines as the minimum efforts a company must take not to have acted negligently (or, put another way, to have acted reasonably). A good starting point for all IT security is to implement security measures to the known standard of care required to avoid liability. While that sounds a bit like a circular statement, let's look at a very simple example. We all know that viruses make their way through e-mail systems all the time. Any company that does not have an enterprise-wide anti-virus software solution in place, that does not scan every incoming e-mail for viruses and other known attacks, has not implemented a reasonable level of care. If a new variant of a virus is released at midnight and your anti-virus vendor doesn't provide an updated signature file until 4:00AM, are you liable for private data being distributed by this new virus via an e-mail leaving your server at 2:00AM? Probably not. What about a case where that e-mail doesn't go out until 9:00AM? Now it's not so clear. Should your virus definition file be updated the instant the anti-virus company releases the update, or is there a "reasonable" window of time during which you cannot be held accountable? Unfortunately that question can sometimes only be answered by twelve people sitting in a jury box—not the ideal place to look for answers to corporate questions. Therefore, if you perform to a reasonable standard in your IT security practices, you will limit your liability to the greatest degree possible.

What Can Be Done?

Fully understanding the risks, as assessed by qualified and experienced counsel, is an essential first step. Taking action that either avoids liability or minimizes the consequences when things go wrong is the next step. The following are some suggestions that might help as you assess your risk and determine your optimal security solutions.

Understand Your Legal Environment

Mitigating legal liability begins with understanding the laws applicable to a company's business. Ignorance of the law is no excuse, and failure to keep pace with statutory requirements is a first source of liability. Working with professionals, whether inside or outside of the company, to track changes in legislation and tailor your IT security policies, is the first line of defense. Careful compliance with laws not only helps reduce the potential for criminal liability or administrative fines, but also demonstrates that all important "standard of care" that might mitigate civil liability as well.

Comprehensive and Ongoing Security Assessments, Evaluations, and Implementation

Working with qualified and experienced legal counsel and technical consultants, a company must identify and prioritize the information it controls that may require protection. That process should include cataloging the specific legal requirements applicable to such information and to the type of business you're in. Next, policies must be developed to ensure that information is properly maintained. As we've discussed, this has everything to do with end user and employee training on security policies, procedures, and security measures. Your corporate IT security plan is only as good as the implementation and maintenance of those security measures, so including the development and implementation of policies and procedures in your corporate IT security plan is vital.

The process of thorough and unbiased assessments, tests, evaluations, and implementation must be ongoing. A static one-shot assessment is almost worse than none at all. Almost equally bad is insufficiently training employees on appropriate policies and procedures for maintaining security measures, or never evaluating those employees on their understanding and implementation of security measures. (The need for employee awareness and training is discussed in Chapter 13.)

Use Contracts to Define Rights and Protect Information

Almost every company has trade secrets—from its customer lists to its business methodologies—that are what afford a competitive advantage. Any protection for these valuable assets will be lost if a company fails to make reasonable efforts to maintain the information as confidential. At a minimum, contracts must be developed that commit employees not to disclose the trade secrets or any information legally mandated to be protected (e.g., individual health care or financial information). These agreements are often most effective if entered into at the time of employment. While this clearly is not within the purview of the IT department, your understanding of the organizational mechanisms that support IT security will help you develop better IT security project plans. In addition, you may find it desirable to advise your Human Resources department, in conjunction with appropriate legal counsel, on what types of policies, procedures, and employee contracts are appropriate in your organization based on the nature and value of the company's data.

Employment policies should reinforce the employee's obligation to maintain confidentiality. These policies should also provide clear guidance on which procedures to use to maintain password security and to responsibly use the information secured on the network. Regular employee training should be implemented to reinforce the notion that these requirements are mandatory and taken seriously by management. Vendors and service providers that may need to review confidential information should only be permitted access to such information under an agreement limiting the use of that information and agreeing to maintain its confidentiality. In most cases, vendors or outsiders should be specifically required to sign confidentiality or non-disclosure agreements to mitigate liability. Hiring any outside consultant to perform a network security evaluation or to review other secret or confidential data without a proper confidentiality agreement in place, could later be found to be sufficient evidence that a company failed to make "reasonable efforts" to maintain information as confidential. In worst case scenarios, this can result in the information no longer being considered a trade secret and therefore no longer entitled to protection.

Use Qualified Third-party Professionals

A key requirement emerging as a critical part of the evolving IT security standards of care is the requirement to get an external review by qualified, neutral parties. These requirements are based on the theory that, no matter how qualified, expert, or well intentioned an organization's IT staff is, it is impossible for them to be truly objective. In addition, there is the ever-present risk of the "fox in the hen house," leaving senior management to wonder whether those charged with creating and maintaining IT security can and will fairly and impartially assess the effectiveness of such security. Finally, qualified and experienced outside legal counsel and technical consultants bring perspective, breadth of experience, and currency with the latest technical and legal developments that in-house staff normally cannot provide cost-effectively. This is not a pitch to get you to run out and hire an outside consultant, but the smart people know when to ask for help, and this might be a good place to start.

Making Sure Your Standards-of-Care Assessments Keep Up with Evolving Law

As suggested above, the legal definition of a "reasonable" standard of care is constantly evolving. Legislators are beginning to take seriously the threats and the substantial economic loss caused by cyber attacks, and to create laws to address these problems. New laws are continually being enacted to punish attackers and to shift liability to companies that have failed to take reasonable IT security measures. Contractual obligations can now be formed instantly and automatically simply by new customers accessing your company's Web site and using your services from anywhere in the world. As new vulnerabilities, attacks, and countermeasures come to public attention, new duties emerge. In short, what was "reasonable" last month may not be reasonable this month. IT security assessments and evaluations provide tools to evaluate and comply with best practices in protecting critical information. However, at best they are only snapshots unless they are performed on a consistent and ongoing basis. Best practices begin with understanding and complying with applicable laws, but security can only be maintained through tracking and implementing evolving statutory requirements. Working with qualified and experienced counsel to follow new legal developments in this fast-moving area of the law and provide advice on the proper interpretation and implementation of legislative requirements can be extremely helpful. In fact, it's becoming increasingly important for mid- to large-sized companies in this ever-changing legal landscape.

Plan for the Worst

Despite all best efforts, nothing can reduce a company's liability to zero (short of closing the doors permanently and even that's not a guarantee). One of the things smart companies have learned is that if (or when) a security breach occurs, the best thing a company can do is get out in front of it quickly. Clearly, part of your corporate IT security project planning work should include incident response to address any security breaches. It should also include your internal and external response plans, including updating security procedures, communicating with appropriate stakeholders, and possibly preparing public statements or press releases. Avoiding liability involves planning for problems (e.g., one class action filed against ChoicePoint alleges that shareholders were misled when the company failed to disclose [for several months] the existence of its security breach and the true extent of the information that was compromised.) Having policies in place to provide guidance to executives in communicating with customers and prospective shareholders may have helped ChoicePoint avoid these allegations.

California currently has a Notice of Security Breach law that was enacted in 2002. As of 2005, Arkansas, Georgia, Indiana, Montana, North Dakota, and Washington have followed suit by enacting some form of legislation requiring disclosure relating to breaches of security, and bills have been introduced in not less than 34 other states to regulate in this area. As of mid-2005, there was no similar federal regulation, although, several disclosure bills have been introduced in Congress. Again, though your job is not specifically to address the legal issues of a breach, your IT security plan should incorporate the development of policies and procedures to be implemented if a security incident takes place. By working with key stakeholders ahead of time, you can reduce the impact of a potential security breach by helping those outside the IT environment understand how you will respond, what steps you will take, and how you will communicate this information within the organization.

Insurance

As more information security breaches occur and are disclosed, the cost to businesses and individuals will continue to rise. In 2002, the Federal Trade Commission (FTC) estimated that 10 million people were victims of identity theft. According to Gartner, Inc., 9.4 million online users in the U.S. were victimized between April 2003 and April 2004, with losses amounting to $11.7 billion. Costs to business from these losses will likely grow to staggering levels in the coming years, and this trend is capturing the attention of some of the more sophisticated insurance companies. Some companies are developing products to provide coverage for losses resulting from breaches of information security. Companies should contact their carriers and do their own independent research to determine what coverage, if any, is or will become available. Again, this may fall outside the scope of your duties as IT security project manager, but is another opportunity for you to add value to your organization by recommending to your executives that they consider evaluating the need for such coverage. In many cases, executives may not be aware of the existence of this type of insurance and as an IT security expert, part of your job is to keep your company's executive team up to speed on this type of relevant information.

This rather exhaustive look at IT security from the legal perspective can cause many IT security professionals to start losing sleep at night. Clearly, there are risks in every aspect of business and IT security is no different. Your company must reduce its exposure to liability by taking reasonable measures, commensurate with best practices in the industry, to secure sensitive information. You can't provide a 100 percent guarantee that your network will never be breached or that your company won't face a lawsuit stemming from a breach. You can, however, develop a thorough IT security project plan, implement it flawlessly, maintain and review security on a regular basis, and train your company's staff on the latest security measures and attack countermeasures. With that in mind, let's return to your corporate IT security project plan.

Corporate IT Security Project Plan Overview

As discussed in the earlier chapters in this book, we're going to look at ISAPs. To that end, we're starting with the overarching plan, the corporate IT security project, which in most companies will include many of the ISAPs presented in subsequent chapters. The plans will all follow the same outline:

1. Define your overarching corporate security strategy.
2. Define the specific problem area (security audit, risk assessment).
3. Define the desired (required) outcome(s).
4. Identify potential solutions.
5. Define project constraints.
6. Define project requirements (functional, technical, legal).
7. Select optimal solution.
8. Define project team.
9. Define project procedures.
10. Define project work breakdown structure, tasks, owners, resources, budget, and schedule.
11. Monitor and manage project.
12. Hand off and close out project.

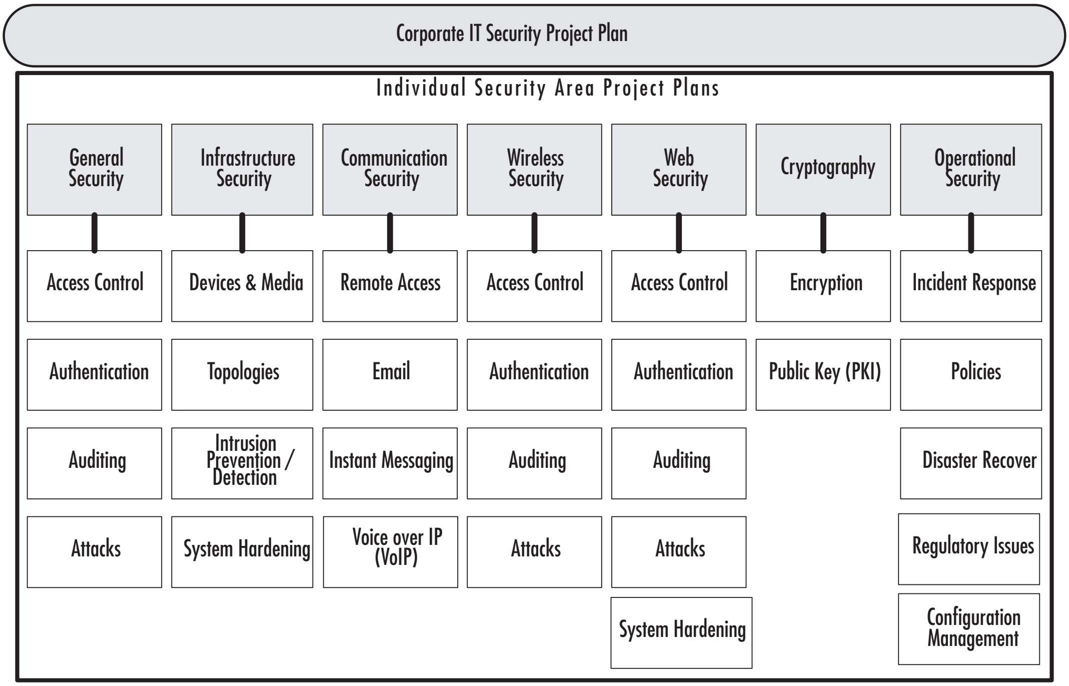
As mentioned in the previous section, you need to start from a clearly defined security strategy. It is outside the scope of this book to step you through developing that strategy, but you can find ample information in various resources, including "*How To Cheat At IT Project Management.*" Defining your strategy in alignment with corporate goals should be the starting point for your corporate IT security project plan. This chapter assumes that you've done that work already. If you haven't, take a step back and define your strategy before developing your corporate IT security plan. You'll save yourself a lot of time and re-work by doing so.

Depending on how your organization works, it's usually advisable at this point to identify your core project team or at least those players you need at the outset to help you develop project parameters. If you work on this by yourself, you may inadvertently be creating two problems. First, you undermine your own ability to develop team buy-in for the project. When people work together to define a project, they are much more likely to feel a sense of ownership and will therefore work harder to make sure the project is successful. Second, you will probably overlook key elements because you can't reasonably expect to know everything that should be included in the project. Getting training, human resources, finance, operations, and legal representatives on the team early will help ensure that your project plan contains all the required elements to meet key stakeholder needs. If you miss this step, you will either deliver a project that falls short of organizational needs, or you'll have to go back and re-work a lot of your project plan. Change is always easier and less expensive to instigate at the outset of the project planning process.

In the IT security world, defining the problem is typically accomplished through a security audit. You may choose to perform a comprehensive security audit or you may choose to audit individual security areas first. Regardless of which way you approach the auditing function, be sure that at the end you have a comprehensive overview. If you work first on the individual areas, be sure you don't leave gaps "between" the individual security areas (i.e., the places where various security areas meet or intersect). If you look at your overall corporate security first, be sure to focus clearly on the individual security areas so you don't miss some area of detail in one of the ISAPs. Either way, you need to take a comprehensive look, but you can choose to go at it from either direction as long as you keep in mind that you need to look broadly and deeply at the current state of security in your organization.

Before we head into the details, let's quickly review the framework for our approach to corporate IT security. If you recall, we delineated numerous security areas in Chapter 1. We've included that same diagram here in Figure 9.1 for your reference.

Figure 9.1 Corporate IT Security Project Plan Components



Corporate IT Security Project Plan

Individual Security Area Project Plans

General Security	Infrastructure Security	Communication Security	Wireless Security	Web Security	Cryptography	Operational Security
Access Control	Devices & Media	Remote Access	Access Control	Access Control	Encryption	Incident Response
Authentication	Topologies	Email	Authentication	Authentication	Public Key (PKI)	Policies
Auditing	Intrusion Prevention / Detection	Instant Messaging	Auditing	Auditing		Disaster Recover
Attacks	System Hardening	Voice over IP (VoIP)	Attacks	Attacks		Regulatory Issues
				System Hardening		Configuration Management

As we move through this chapter, keep in mind that we're focusing on the overall corporate IT security project plan, but that these same elements will also be used in subsequent individual security area project plans. You may have additional ISAPs defined for your organization and, if so, you can utilize this framework to develop project plans to address those specific areas.

Corporate Security Auditing

Before you can embark on any IT security project, you need to understand the current environment. As we've stated several times, in project management, you should start with a problem statement. The problem statement for corporate security can be as general as, "We currently have no clear understanding of our network's vulnerabilities." However, the more specific you get, the better your solution will be. If you say, "Our network consists of servers, network storage devices, end user computers, Web services, wireless access and sensitive corporate and customer data. We do not have a detailed approach to securing these network resources." You are getting closer to defining the real problem and closer to identifying the real need. One way to develop a solid security project plan problem statement is by conducting a thorough security audit. Since knowing your starting point is the logical genesis of any security plan, we're going to delve into the details of conducting a security assessment or audit. You can conduct your assessment as one of the first major objectives of your corporate IT security plan, or you can create a separate security assessment and auditing project plan to be conducted and concluded prior to the development of your corporate IT security project plan or any of your ISAPs. Either method is acceptable as long as your projects build upon the results of your audit. In this chapter, we'll use the terms *assessment* and *audit* interchangeably.

Auditing means different things to different people but we'll use a definition commonly used in the IT security world: a thorough and methodical review of systems and technologies focused on finding vulnerabilities. Some companies hire outside security consultants to assist with their security auditing. If you choose to perform your own network security audit, you're going to need several tools and a lot of expertise to do so effectively. You'll also need one or more people on your team to volunteer to think like hackers so you can discover vulnerabilities hackers would likely exploit.

Business Intelligence…

Ethical Hackers?

The term “ethical hackers” seems like a bit of an oxymoron, however, it’s actually a growing field of interest these days. In order to effectively thwart hackers, you need to have the same or better skills as hackers. There are numerous companies that train people to hack systems so they can use their skills for the benefit, not detriment, of the company. Numerous organizations provide ethical hacker training and certification programs and you can find many listed using a quick online search. These courses teach participants to use the same tools, techniques, and thought processes that hackers use in order to exploit vulnerabilities and to force their way into computers, networks, and other electronic corporate resources. However, there’s good news and bad news. The good news is that having these skills on your IT team can be valuable in keeping your corporate network safe. The bad news is that it’s always a bit unnerving to teach your employees how to hack a network. However, if you look at the open source model for software development, you find a similar logic. Open the knowledge to many and you have a better chance of exposing and addressing vulnerabilities. And, while you can send your employees for training, you can also hire an outside consultant who is a certified ethical hacker to teach your IT staff how to hack. Remember, though, your employees may choose to learn on their own, so keep all of your options open and keep an eye on your network through various, independent methods.

Choosing A Target

Hackers, like robbers or car thieves, will attack the easiest targets first. For example, in the case of wireless networks, hackers will certainly take an unsecured wireless network over a protected one any day. Just like the car thief, the easiest cars to steal are ones that are (in this order):

1. Running with the key in the ignition
2. Unlocked
3. Locked
4. Locked and have a visible security device (e.g., a steering wheel lock),
5. Locked and have an alarm system
6. Locked and have an alarm system and an engine-disabling device

For a hacker, the easiest networks to hack are those that are unsecured. However, corporations can be rich targets for hackers, either because of the data on the network (financial, personal identification, and so forth) or because they can access trade secrets, Research & Development, and other confidential corporate data. The potential payoff makes it worth the effort. Finally, there is the "hacker of convenience" who hacks into a network just to see if he or she can; sometimes it just boils down to bragging rights. Therefore, your goal in network auditing is to find the vulnerabilities from easiest to hardest (just like a car thief). If you plug the obvious holes, you're better off than doing nothing, but you're not secure.

Business Intelligence…

The Best Defense is a Good Offense

What's the best way to secure your network? By taking both a defensive and offensive position. The defensive position consists of all the things you do to secure your network, from requiring strong passwords, to controlling and auditing access to key files, to hardening your servers. It's like locking the doors and windows on your house to make sure it's secure before heading off on vacation. However, that's not enough in network security. Hackers, like professional burglars, are scoping out your network just looking for an opening. In network security, you have to also take an offensive approach and attack your network from as many different angles as possible. Not only do you have to think like a

Continued

hacker, you have to be as creative as a hacker and think of different ways to attack your systems. This is one reason outside consultants can be helpful; they aren't well-versed in your systems and will come in with a fresh perspective and without any pre-conceived notions about how your system does (or does not) work. He or she will be able to examine elements of your network security you and your team may overlook.

Why Security Fails

An important aspect of understanding how to secure your network comes from understanding why network security fails in the first place. It's not just a matter of an unused port being left open on a server or a default setting being left in place. Security and security failure depends on a number of interrelated aspects including:

- Improper configuration
- Failure to update
- Faulty requirements
- Human factors
- Policy issues
- Incorrect assumptions

Improper Configuration

Improper configuration is one of the first areas IT managers think of when they think of how security can fail. Failing to change settings from the default or out-of-the-box settings is a major source of security risk, since every hacker in the world has access to the same data you do when it comes to default settings. Those of you familiar with Microsoft Windows Server operating system know that the major change to the 2000/2003 versions is that the default settings came locked down rather than fully open. In older versions, Microsoft assumed you'd lock down any functionality you didn't want to use or didn't want users to access. However, that left many open doors for attacks. In the latest versions, the out-of-the-box configuration comes locked down and you have to deliberately enable key functionality. This is clearly a better approach to security but it's not a cure-all. Other equipment including routers and wireless access points in particular, come with default settings that many companies fail to change during normal installation and configuration.

In addition to using default settings, there is also the chance for simple error when making changes to configuration settings. Other times, the settings are properly configured but the resulting configuration has unintended consequences elsewhere in the system. These are the kinds of issues a solid security assessment plan will try to locate and address.

Failure to Update

Anyone working in network security these days is well aware of the need, or rather the requirement, to keep systems up-to-date. The adage that "two heads are better than one" comes into play from both sides of this issue. Hackers are increasingly collaborating together and are getting smarter and more sophisticated. On the other side of the issue, various hardware and software vendors are also working harder to maintain security. Since attackers are never going to stop trying to improve their chances of getting into your system, you have to stay one step ahead through keeping systems up-to-date. If you don't have a comprehensive plan in place for keeping operating systems, applications, and security applications (anti-virus, anti-spyware, and so forth) up-to-date, your entire network is vulnerable. Part of your assessment should include your current update plans.

Faulty Requirements

Functional and technical requirements are the foundation of any technology project. Whether building a server, designing a rocket, or constructing a solar power generator, all require well-designed requirements. If the requirements are faulty in any way, you have a poorly designed system. In the case of network security, requirements tend to build one upon the next, creating a layered effect (e.g., the requirements for the server hardware, operating system, applications, communications protocols, network routers, and firewalls combine to create the security that impacts that one specific server. If anywhere along the line those requirements are poorly conceived, designed, or executed, you have a potential security gap. This was the case about ten years ago when some Department of Defense systems had serious security vulnerabilities. It wasn't that the vulnerabilities were new or unique, it was that the systems were poorly engineered and long-term plans for remediation were needed. If they had fixed the issues immediately, it would have had a dire impact on the mission. Faulty or poorly designed requirements can create a serious problem at many different levels of network security. Each of your ISAPs as well as your corporate IT security project plans should include functional, technical, and legal/compliance requirements to ensure that you are addressing security at the most basic level.

Human Factors

In network security, humans are the weakest link. Human behavior is fairly predictable. We don't remember complex passwords very well, so we write them down. If we don't have to use complex passwords, we use ones we can easily remember so we don't have to write them down. Unfortunately, these end up being passwords that can be easily guessed or found through a dictionary search. Using your pet's name or your wife's birthday helps if the attacker doesn't know you, but a large number of security breaches happen inside the organization. If your user account has administrative privileges and you use your wife's birthday as your password, how hard is it for someone in your organization to hack into your account? If you use a word found in the dictionary, a computer could hack the account in about 20 seconds, on average. Users, developers, managers, and IT administrators all fall victim to shortcuts for remembering passwords, and there are those in the industry that believe that IT administrators are the single largest security vulnerability.

There's also the issue of social engineering, where users are persuaded or tricked into giving up their usernames and passwords. More sophisticated forms of social engineering have spawned "phishing" and given the proliferation of the practice, one would have to surmise that phishing is successful enough to be worth the effort. In many cases, it's just easier to ask. You'd be surprised how often people will divulge their passwords if the request appears appropriate. Have any of your IT staff call anyone in your organization and ask for their password and see how often someone is willing to divulge it.

Finally, there is the aspect of physical security. Laptops are stolen, users leave their desks unattended, and network resources are left unsecured. Physical access to a server is absolutely the best way to hack it. Sitting down at the receptionist's desk that's logged on to the network might yield useful information to an attacker. Your network assessment needs to account for the human factor in all areas of security.

Policy Issues

The quality and comprehensiveness of your security policies and practices is at the heart of your network security. Your policy should be created in conjunction with your human resources staff and your legal counsel to ensure that you're creating policies and procedures that make sense for the whole organization. Legal counsel helps ensure policies meet legal requirements, both from a human resources perspective and also from a legal risk mitigation perspective. Your policies and procedures need to be strong enough to meet standards of "reasonable care," but they also must conform to standard human resources practices.

We've discussed the importance of involving key stakeholders in your project planning process right from the start. This is one key area where outside assistance from human resources and legal can help tremendously. If security policies are mismatched to the organization, there's a very high chance that compliance will be low. The major problems users run into with security policies is that they're:

- **Too Stringent** Requiring a 35-character complex password, multiple logins, and so on. Will usually cause the user to find ways to circumvent the policy.
- **Too Old** Outdated security policies undermine the credibility of the policies that are still up-to-date. Asking users to sort

through and determine which are relevant and which are not creates an inconsistent approach to security policies, which leads to security risks.

- **Unread or Unused** Security policies that are not read or enforced by the IT staff, management, and human resources are useless. It doesn't matter how many locks you put on the door if you leave the door wide open.
- **Vague or Unclear** Policies that are vague, confusing, contradictory, or that provide no clear direction on how users can comply are worse than no policies at all. If users do not understand how to comply with security requirements, they will usually resort to doing whatever they need to do in order to get their jobs done. That often means circumventing security best practices out of desperation. If users are told they cannot transmit a patient's medical data across unsecured lines or without encryption but they don't know if their lines are secure or how to encrypt a file, there's a good chance they won't comply.

Your security assessment should include reviewing, modifying, updating, and deleting all existing security policies so that the resulting set of policies is up-to-date and relevant to the current (and near future) security environment for the network. You should also make sure that your policies are clear enough that users understand and know how to comply with security policies.

Incorrect Assumptions

The difficulty about assumptions is that we don't always know we're making them, and that's the root of security issues. If we assume users behave in a particular way and we're wrong, we potentially have a security hole. If we assume a particular set of configuration settings will result in a particular outcome, we've created a potential security hole. If we assume that the technology works in one way and we're wrong, we've left the door open to attack. Testing assumptions is an important part of your security assessment process. Unfortunately, it's not always easy to see what we're assuming. There are several ways to address this including consciously asking, on a regular basis, "What assumptions are we making here?" involving those outside the IT environment to provide a fresh perspective and unbiased approach, and hiring outside experts who come in without those same assumptions in mind.

For example, suppose someone wants to get at your customer database. The attacker knows your company has a large online store with millions of transactions flowing through on a monthly basis. The attacker looks on your company Web site and eventually is able to cause the database server to generate an error that gives the attacker the information he or she was looking for. The attacker uses the result of the database error to inject code that enables him or her to hack further into the system. He or she gives themselves administrative privileges, covers their tracks, and sits in the comfort of his or her home grabbing any database information he or she wants. You may have looked hard at your Web server and made sure that it was secure and that customer transactions were secure and assumed you were all set. These are exactly the kinds of assumptions attackers hope you'll make.

Another assumption we discussed earlier in this book is the assumption that the proper steps were followed when implementing various security measures. If you simply assume the proper steps were followed and completed, you leave open the possibility that these measures were not properly completed. Using completion criteria for each task (see Chapter 6 for more detail) will help ensure that each security task is completed successfully and per your security project plan. Using completion criteria and spot checks on various security measures will help you to know, rather than assume, that your security measures have been properly implemented.

Corporate IT Security Project Parameters

After completing the risk assessment and impact analysis for your corporate IT security project, you should have a better idea of the problem(s) you're trying to solve and the desired outcomes. These should be well-aligned with your enterprise-level security strategy. If not, you'll need to circle back through the process and locate and address any disconnects. At the conclusion of this process, you should document both the problem statement and the outcome statement. This can be a relatively short few sentences just to make sure you've clearly identified the problem you're trying to solve and that you've identified the outcome you want to achieve. There will always be a balance between security and cost and between security and operational efficiency, and this is the place to begin to find that balance.

Project Objectives

Your corporate IT security solutions should include all of the security areas you need to address. Figure 9.1 shows several common security areas that are likely to be a part of your plan. These include general, infrastructure, Web, wireless, communication, and operational security, among others. You may find that you want to slice and dice your security areas differently than we have here. That's fine as long as you take a logical and comprehensive approach to the wide variety of topic areas you need to cover, and don't inadvertently omit anything.

Your potential solutions include all of the security topic areas you want to cover. We also know that in the real world of corporate finance, there's a good chance that your complete list probably falls under the label "wish list" rather than "to do list." Since you will likely be forced to make some compromises and tough choices, it's important to start with your ideal list and pare it down from there. Once you've identified your ideal solution, you need to circle back and see how it compares with your project constraints starting with the scope, time, cost, and quality.

Project Parameters

All projects have four parameters: *scope*, *schedule*, *budget*, and *quality*. As we've discussed, there is a relationship among these parameters that must be addressed at the outset of any project planning process. You can create a smaller project scope by phasing your projects and identifying ISAPs within the corporate IT security project plan. Your overall plan and your ISAPs will each have the four parameters and will move independently.

For example: Your corporate IT security project may have a schedule of 12 months and a budget of $500,000. Your communication security plan, which includes e-mail, instant messaging, Voice over IP (VoIP), and remote access, has a schedule of 30 days and a budget of $10,000. Clearly, the 30 days is part of the 12-month schedule and the $10,000 is part of the $500,000 budget. However, the priority for your corporate IT security project might be time —it must be completed in 12 months. On the other hand, your priority for your communication security plan might be budget—you don't care if it takes two months or even three months, but it can't cost more than $10,000.

This is one of the reasons it's helpful to break a project down into smaller sub-projects. You can adjust priorities for the sub-projects (in our case, the ISAPs) in a manner that drives your overall goals and objectives. This can be especially helpful if you believe that another segment of your corporate IT security project plan could take more time than allotted. In that case, you might need to allocate more funds to hire outside contractors to come in and assist in getting the job done. By having both the overall plan's project parameters and priorities identified and by working with the ISAPs, you can build in a bit more flexibility than you might have otherwise.

Scope

The scope of your corporate IT security project plan includes the scope of all the ISAPs (if you choose to break your projects out in this manner), but that's not all it should include. The corporate IT security project, in some sense, is the mortar that holds the bricks (ISAPs) together. Each individual security area is important, but without a holistic approach to security, you're bound to have gaps between these areas. The scope of the corporate IT security project should reflect this need. You can include the scope statement from each of the ISAPs and you may want to include the following items as well:

- Comprehensive review of network systems security
- Comprehensive test plan for systems vulnerability
- Vertical security assessment and hardening
- Horizontal security assessment and hardening
- Perimeter security assessment and hardening
- System-wide IT security policies and procedures
- Corporate IT security policies and procedures
- System-wide IT emergency response plan

At the risk of being repetitive, these elements should take a system-wide or corporate-wide look at the same areas that will be addressed in one or more of your individual security area plans. In some cases, there is overlap and in other cases there are gaps. The goal of the corporate IT security project plan is to ensure that any areas that overlap are appropriately resolved and any gaps that exist are addressed. Think of the corporate IT security project plan as your last line of defense.

Another useful way to look at the scope is to look at the physical elements of your network. How many locations does your company have? How many buildings does that entail? How many logical or physical subnets are there? How many servers? How many desktops? How many users? Are you planning on addressing every aspect of your IT security in this plan or are you going to take it in phases? If you remember the project management guideline that smaller projects tend to be more successful than larger projects, you can see that properly setting your scope is key to success. If you determine that your corporate IT project must address every aspect of IT security, you will definitely need to break it down into smaller ISAPs. If your network security is relatively good and you simply want to make sure things stay up-to-date with the latest threats, your scope may not need to be quite as extensive.

Finally, you might look at your network both horizontally and vertically. A vertical approach looks at a single host or single host type and looks for all vulnerabilities that might impact that host type (e.g., look at all of the desktop systems running Microsoft Windows XP Professional and look for all vulnerabilities, threats, and remediation strategies related to that operating system and those devices.) This is defined as the scope of your corporate IT security project or the scope of just Phase One. A horizontal approach is useful for spanning various platforms and might include looking for any device that could be vulnerable to a Transmission Control Protocol/Internet Protocol (TCP/IP) port scan or a Denial of Service (DOS) attack. This approach could be used to define the scope.

Ultimately, you want to review all systems top to bottom and side to side, but if you've recently completed a number of security measures or if a comprehensive corporate IT security project plan is outside of the financial means of the company, you may choose to scale it down using these various elements of scope.

Schedule

There are a number of elements regarding the schedule of a corporate IT security project and the related ISAPs. The overall schedule may be dictated by a planned, future event such as the company going public via an Initial Public Offering (IPO) or a requirement to be compliant with a particular set of regulations by a certain deadline, or maybe by a deadline determined by the executive team. These are external constraints that must be considered as you build your project plan. If schedule (time) is your top priority, you already know that something else will have to "give" if the project runs into problems (which almost all projects do at one time or another). In this case, you need to plan for the possibility that you will need to add more people to your project if work is delayed for any reason. You also need to be ready to scale your scope back a bit if you fall behind schedule. The corporate IT security plan will have to be the most flexible, because it will have to accommodate the changes to all the underlying ISAPs and it will also have to provide a thorough, integrated approach to corporate security as a whole.

In addition, you may set high-level target completion dates for various elements of your project and then set your more detailed schedule based on the ISAP schedules you develop. For example, you may choose to complete a Web security project plan first, because you know your Web systems are most vulnerable at this time. You expect that project to take two months to complete. You might choose to begin the planning stages of your infrastructure project plan, because you want to begin implementing it as soon as possible. You may also be able to utilize different members of your IT staff so that you can run these projects in parallel. These are the kinds of things you can decide on regarding your schedule when you take a holistic, system-wide look at your security initiatives.

Budget

Determining the budget for your corporate IT security project can be the most challenging aspect of developing your corporate IT security plan. How much it will cost is often a function of how much it can cost, meaning that your security budget may well be set by corporate or IT budget constraints. If your budget question is answered for you, then you'll need to reverse engineer your budget to determine just how much security you can get for some set number of dollars.

Phasing your security projects can also help when overall cost is not as much as an issue as the timing of cash flow. You'll need to determine if your costs are primarily internal or external. Internal costs are those such as labor costs for staff, loss of productivity (which often isn't captured in any organization), and any other cost that essentially involves shifting money around in accounts. External expenses are the ones that often have to be timed and explicitly approved. Purchases including new security hardware, software, or external labor often require specific sponsor approval for the expenditure if it exceeds a certain threshold. Often you can negotiate a higher overall budget for your corporate IT security project by negotiating the budgets for the smaller ISAPs individually. Beware of one trap of this approach. Sometimes you'll negotiate a budget for an ISAP such as infrastructure security and, whether accidentally or intentionally, it is construed as your entire security budget. Be extremely clear in your communications that if you choose to negotiate individual project plan budgets that you're talking about a subset of your total security needs. If you are painfully clear about this, you'll avoid problems down the road, but you will likely have to answer the question, "How much will the whole thing cost?" Although you may not know (or may not want to say at that moment), you can briefly lay out your approach to managing the costs by discussing your overall corporate IT security strategy. In some companies, this piecemeal approach to budget expenditures is an effective way to reduce organizational resistance to security spending. In other companies, this approach could be viewed as manipulative or underhanded, in which case you should find a more acceptable method of presenting your budget needs.

Quality

Although even one security breach can be devastating for an organization, the cost of guaranteeing zero breaches can be astronomical. You'll have to find the balance between the quality your organization requires and the cost it can afford. In many cases, there is a direct relationship between the level of quality (or the tolerance for breaches) and the cost of the project. Therefore, if budget is your top constraint, you'll most likely need to adjust your scope or your quality. Reducing quality is not as bad as it sounds. Adobe Photoshop is a great program, but it's pricey if all you want to do is view pictures from your digital camera and add captions underneath. Less expensive programs offer lower quality, but if that's all you need, why pay more? The same holds true for your corporate IT security quality level. Deliver the highest quality you can afford, and recognize that no solution is ever perfect. Define what level of risk you can afford to operate under and let that be your guide to quality. If the level of quality your organization requires is higher than your budget allows, you will have to build a business case for increasing the budget. You may find an ally in your legal department or a legal representative who can help explain the cost of the risks (and consequences) that you're trying to mitigate.

Requirements

Every IT project should have well-developed requirements that define the boundaries of your project. Your scope statement states what is and is not included in the project, but the requirements provide the details for those scope statements. Functional requirements answer the question, "What should this project accomplish?" A good example for corporate security might be that the functional requirement specifies the implementation of a stronger authentication system, because a recently passed law or regulation requires it. The functional requirement says the project must include a "strong authentication system as defined by Regulation 123."

Technical requirements describe *how* you will accomplish the functional requirements. They are typically quite specific and binary: either it is or it isn't; either it meets specifications or it doesn't. A stronger authentication requirement might provide very detailed technical specifications for smart cards or biometric hardware in very specific language. Technical requirements are server processor speed or hard disk capacity (i.e., they are clear, tangible, and relatively easy to define.)

Project management is an iterative process—you often have to circle back to add detail as information becomes available. Requirements may be known at the outset of a project, in which case they should be included. However, it's also common for new or additional requirements to be added as you move through the definition and planning phases of your project. You may not know that strong authentication is a requirement until you've done a risk analysis or audit. You may not know that you need a biometric system for authentication until you've completed some other part of the project work or read a new section of a regulation. The key is to define what you're aware of and revise the project plan as details become known. That doesn't mean that you're shooting at a moving target—just the opposite. Pin down as many details as possible, knowing that as you gather data and do your research, you'll develop finer levels of detail. Don't get lost in the spin cycle, but do refine your data as you gather additional information.

Projects may also have some sort of organizational requirements (e.g., a particular security measure must be compatible with screen readers used by visually impaired employees, or the security measures do not violate employee privacy as defined by the organization. These typically should be translated into functional and technical specifications, but they can also be noted separately as organizational requirements to ensure they receive the attention they deserve.

Finally, IT security projects will have legal and regulatory issues that need to be defined as requirements. Again, these can be listed as legal, regulatory, or compliance requirements to give them needed visibility, but they ultimately should be translated into functional and technical requirements for the project.

Key Skills Needed

Although we touched on this in earlier chapters, this is a good time to reiterate the basics. Your corporate IT security project team should include people from all areas of your organization with both technical and non-technical skills. You can create a list of the technical skills needed for each of the ISAP projects, and roll your skills list up into your corporate IT security project plan. However, you might need to take a bit more time identifying the non-technical skills needed (e.g., you don't always need technical people to create security policies that include physical computer equipment security policies, e-mail, and Internet and training policies, and you don't always need technical people to create and deliver related user training). The following is a list of skills you may need for your corporate IT security plan:

- Technical
- Communication
- Training

- Policy development
- Technical and non-technical writing
- User requirement development
- Financial (to create the budget)
- Legal (to advise on various aspects of your project)
- Human Resources (to help develop user guidelines)

From the technical side, there are numerous skills you're likely to need. The core skills needed to assess security (which are usually the same skills needed to implement security solutions after assessment) are operating system, network, application and programming skills. These skills are often found in two different groups of people. Most of your IT staff can be divided into "network guys" and "programmers." Your network experts are the ones you turn to when you have a router outage, a server configuration issue, or a new application to install. Programmers typically look at the world in a different way; they're usually not the ones you want configuring your database server, but you do want them writing and testing the scripts. Understanding the core skills of your IT staff and where they're most appropriately applied in your IT security project plan is critical.

Most technical skill sets are either deep or broad and it's not too common to find someone whose skills are both. If someone knows routers inside and out and can list off soft switch settings for every Cisco product ever made, he or she most likely won't be able to tell you the best way to configure access control lists for the database. In fact, your department likely has a mix of generalists and specialists specific to the jobs you've needed to get done in the past. However, that doesn't necessarily help when you're looking the skills needed for your corporate IT security project. A skills assessment may be necessary before you undertake your security project and you may need to train staff or hire expertise, which should be reflected in your project budget.

Operating System Skills

You should have at least one person on staff with deep operating system expertise for each operating system deployed in your organization. If you're running Windows, Linux, and Apple, you ideally should have experts in each of those areas who are well-versed in securing each of those operating systems. Your expert(s) should have a detailed understanding of the operating system's subsystems, with special emphasis on the security subsystems. Operating system fundamentals change slowly, so this is one area where in-depth study will pay off. This is also an area where you should have good bench strength.

Create a list of all of the operating systems deployed in your organization, and make sure you have one or more experts on staff that can assist in developing, implementing, and maintaining your corporate IT security plan. Excellent training in these areas is widely available and a good investment to ensure that staff skills in this area are up-to-date.

Network Skills

As an IT Manager or IT Security Project Manager, you probably recall the Open Systems Interconnection (OSI) model in name only. However, if your job is to secure the network, the OSI model should be permanently etched in your brain. Understanding what goes on in the network at Layer 2 and 3 is critical to security, because that's where most of the routing, switching, and security controls operate. Another network skill you should have on your IT staff is Internet Protocol (IP) expertise, people who can count and add in hexadecimal format in their sleep. They should be familiar with subnetting, supernetting, IPv4, IPv6, IP telephony (VoIP), and all of the other ways the IP is implemented, used, and configured in the enterprise.

Part of your corporate IT security project plan should include a list of the network skills needed based on the type of systems you have in place and what you're planning to implement in the near future.

Application Skills

Staying up-to-date on application skills can be a challenge, because unlike operating system or networking data, applications rarely stay the same from version to version. The core application doesn't change much, but enterprise-wide applications are typically complex programs and when something changes in one area, it ripples through the application at lightening speed. This creates a security challenge, because on one hand, you don't know exactly how the latest updates impact the application and its security (i.e., did the developers do a good job testing security on this latest release?) and you also don't know exactly how the application changes might impact your business operations and security (i.e., how well-versed you are in the latest nuances of the application and how it impacts your system security).

The application skills your organization requires are database skills and Web application skills. If you don't have these skills internally, you should add them to your requirement list so that the next time you hire someone, you will hire them with these skills in mind. Database and Web-related security are two areas that hackers like to attack, so be sure you have the requisite skills in this area.

Identify the applications in your organization and check to see if you have the necessary skills. If not, seek out vendor training so that you can adequately secure your company's applications.

Security Tools Skills

Depending on the scope of your corporate IT security project plan, you may or may not need to delve into the detailed world of specific security tools. In later chapters, we take a look at various security tools. Some are simple scripting tools and others are hardware devices. Depending on your project plans, you may purchase these tools and train staff to use them, or hire external contractors who have the tools and the expertise. The decision will primarily hinge on the potential payback on the investment. If you're going to need these tools on a regular basis, it makes sense to make the investment in the tools and training. If a tool will only be used occasionally, it might make sense to hire a contractor, who can bear the time and expense of staying up-to-date. You can hire their expertise for less than it would cost you to develop that expertise in-house.

There are many training methods available including online courses, workshops, and boot camps that train staff how to use security tools. One thing to consider, though, is that not all courses teach participants to think like hackers, and using the security tools without the mindset of an attacker will likely yield less than optimal results.

Programming Skills—Compiled Languages

In order to perform security testing, you should have programmers on staff that are conversant in various compiled languages. Is it absolutely necessary? No, but it's often helpful to create automated testing procedures and to understand how to read source code and see what's going on beneath the covers. C and C++, C#, and Java are the primary languages in use, although there are others. C, C++, and C# are not the same languages. Both C++ and C# are object-oriented languages; C is not. However, all share similar syntax and semantics. C# is a relatively new variation and is used primarily in Web applications and Web services. Java is also an object-oriented language, developed by Sun Microsystems, and is used across a wide variety of platforms and devices.

Determine what security projects you're going to undertake and whether you'll need these programming language skills in-house. In some cases, you may want to hire the programming expertise you need from an employment agency, but be careful about what you provide to the contractor. You could be hiring the guy who opens the back door on your system.

Programming Skills—Scripting Languages

Scripting languages (also called interpreted languages) are often used for a variety of administrative tasks, so chances are your IT staff has a variety of scripting skills. Take a full inventory of all scripting skills in your department. This will not only help you match skills to need, but it might also prompt a few creative ideas for how to approach various security tasks.

The most commonly used scripting languages these days are Microsoft's Visual Basic Scripting Edition (VBScript), JavaScript, Python, and Perl. VBScript is typically used to automate various administrative tasks, especially in the Windows environment. It's also widely used on the client side of Web services. JavaScript is also used in client side code on Web sites. VBScript is specific to Microsoft and JavaScript works across the Microsoft, Unix, and Linux platforms. Python is also an object-oriented scripting language that is used extensively in the Google search engine. Python runs on Windows, Linux/Unix, Mac OS X, OS/2, Amiga, Palm Handhelds, and Nokia mobile phones. Python has also been ported to the Java and .NET virtual machines. Python is distributed under an OSI-approved open source license that makes it free to use, even for commercial products. Python is slowly replacing Perl, though there are still many Perl scripts running in the world.

Key Personnel Needed

Once you've identified the scope of your project and the skills needed to successfully complete your corporate IT security project plan, you can start mapping the specific people to their skills. For example:

- **Communication** - Jesse (IT), MaryAnn (HR)
- **Training** - Lisa (IT), Fernando (IT), Sonali (Training)
- **Policy development** - Bill (IT), Marcos (HR)
- **Technical and non-technical writing** - Lisa (IT), Sonali (Training), Ming (HR)
- **User requirement development** - Luisa (Business analyst), Ming (HR)
- **Financial (to create the budget)** - Deepak (Finance), Lisa (IT)
- **Legal (to advise on various aspects of your project)** - Larry (Legal)
- **Human Resources (to help develop user guidelines)** - Nels (HR), Ming (HR), Fernando (IT)

You can see from this list that there are two names that appear multiple times—Lisa from the IT department and Ming from HR. Are you sure that Lisa and Ming will be available? Can Fernando cover for Lisa in any of these areas? As you develop your list of needed personnel, also create a viable list of alternates. If these people are not available and are truly needed, your project will be delayed.

Notice we didn't list any of the technical skills or technical personnel needed. It's assumed you'll do this in each of your ISAPs and roll it up into your corporate IT security plan. However, you may need or want to include additional skills and personnel to your corporate IT security plan, if you want to provide a higher level skill set to the mix (e.g., an outside security consultant to review your overall plan or someone with a systems integration testing background who normally works in a different department or division).

Project Processes and Procedures

The overarching question is this: What processes and procedures do you need to implement to manage your corporate IT security project plan? The answer lies in your approach to your corporate IT security plan. For example, if you choose to break your corporate IT security project plan down into the underlying ISAPs, how will you manage the timing, resource allocation, reporting, and scheduling of these projects? How will you manage resource conflicts? How will you know if you're over budget or behind schedule?

The key to developing your project's processes and procedures is to look at what you've defined thus far. What does your scope look like? How are you organizing this project? Next, you'll need to find your standard project processes and procedures and review them. Are they appropriate to this project? Do they contribute to or compromise overall security? For instance, for some projects, you may want people to collaborate on particular sections of the project, but in a security project, you may want people to work independently so they can test each other's solutions. Having one person develop the solution and another devise the test of that solution can sometimes yield better results.

As part of the organizational security ISAP, we'll discuss both organizational security policies and procedures and emergency response policies and procedures, so we won't cover them here (see Chapter 13). The processes, policies, and procedures we focus on in this section are those needed to effectively plan, implement, monitor, and manage your enterprise-wide IT security plan.

In addition, you may want to implement additional procedures related to security projects including:

- Require that IT staff create special user accounts for testing so that employees who have been given permission to test security can be recognized and monitored on the system. These accounts can later be deactivated or used only in cases of security testing. This can help separate out legitimate testing from insider hacking.
- Develop specific procedures for testing security and for recovering from any unintended consequences of that testing. Sometimes pen testing (or other security testing) breaks something in ways you couldn't foresee. Having specific recovery procedures in place will help mitigate project risk.
- Develop procedures to prioritize security breaches found during testing.
- Develop procedures for notifying key staff of serious security holes found and the appropriate measures to take. The last thing you want is for one of your staff to find a significant security hole and be told, in essence, "That task isn't scheduled for another month. Remind us later." Your security procedures should include escalation and notification procedures for serious security issues uncovered during the security project.
- Create policies and procedures for emergency response teams in the event of a real security breach.

- Develop policies regarding how IT staff handles the sensitive information discovered during security assessments and audits. Remember, discovery of security holes can lead to legal liability if reasonable measures are not taken to address those shortcomings.
- Develop policies detailing how and when to perform complete backups and how to restore systems. Always perform complete backups of critical systems before performing any audit or test activities. Also ensure that backups are tested with sample restores prior to auditing activities.

There may be many other security-related policies and procedures you want to employ in order to successfully plan, implement, and run your corporate IT security project plan, but this will get you started thinking along the lines of things that are specific to security projects.

Project Work Breakdown Structure

Recall that your work breakdown structure (WBS) is created from your project objectives. Typically, you'll have three to five high-level objectives to start with. In the case of your corporate IT security plan, you'll probably end up incorporating sub-plans (ISAPs) into the master plan. To that end, you may not decide to list out each of the ISAPs for your project, but instead include those as one high-level objective. Let's look at a few examples of how you can define your corporate IT security plan. Remember that if you don't already have your core project team working with you on defining your project, there's no time like the present to get them involved. If you define your WBS without key stakeholder and subject matter expertise input, you'll have a lot of rework on your hands later on.

WBS Example 1

1. Develop enterprise security strategy
2. Perform enterprise-wide security audit

3. Implement individual security area plans based on audit results
    - 3.1 Develop and implement the Infrastructure Security Plan
    - 3.2 Develop and implement the Web and Internet Security Plan
    - 3.3 Develop and implement the Communication Security Plan
    - 3.4 Develop and implement the Wireless Security Plan
    - 3.5 Develop and implement the Cryptography Security Plan
    - 3.6 Develop and implement the Operational Security Plan
4. Perform cross-functional security review
5. Develop ongoing security maintenance procedures

In this example, developing the security strategy is the first major objective of your corporate IT security project plan. Some might argue that this step should be completed prior to developing your corporate IT security project plan, but if rolling it into your project planning process is helpful, there's no harm in doing so as long as it's completed before moving into the development of the remaining four high-level objectives (which translate into your top-level tasks in your WBS). Notice that Task 3 is a high-level placeholder for ISAPs. Several are listed underneath Task 3 for illustrative purposes only. One quick reminder is that best practices dictate that task names use a verb and a noun format so they are somewhat descriptive. Let's look at another corporate IT security WBS you might use as a starting point.

Work Breakdown Structure Example 2

1. Develop RFP to hire an outside security consultant for an enterprise-wide security audit
    - 1.1 Define RFP parameters
    - 1.2 Develop a list of companies from whom to solicit RFP responses
    - 1.3 Issue a RFP

  1.4 Evaluate RFP responses
  1.5 Hire an outside consultant
2. Perform enterprise-wide security audit
3. Implement security recommendations based on audit results
  3.1 Develop ISAPs
    3.1.1 Develop and implement Infrastructure Security Plan
    3.1.2 Develop and implement Wireless Security Plan
    3.1.3 Develop and implement Operational Security Plan
  3.2 Implement, monitor, and manage defined ISAPs
4. Develop ongoing security maintenance procedures

In this example, you've decided to hire an outside consultant to perform a security audit. From those results, you will develop your individual security plans to address the specific areas or vulnerabilities identified by the consultant. You may develop those plans with or without the consultant, and you may decide to implement and manage those projects with or without the consultant. Those are choices you can make as you move through the process based on the unique characteristics of your organization, your IT staff's capabilities, and your relationship with the consultant. However, regardless of who does the work, you are the project manager and should actively manage the process. In most cases, it is not advisable to hand off responsibility for the project to an outside consultant, unless you are explicitly hiring them to come in, assess your security needs, develop the security project plan, and implement the resulting plan. There are some instances when that might be advisable, but as a general rule, you should maintain control of the project, because you'll be held accountable for the results when it's all said and done.

As part of your WBS, you'll want to include the specific security areas you plan on addressing. You may have to circle back through your planning process to add detail once your security assessment or audit is completed. If the assessment or audit is conducted prior to planning your corporate IT security project, you most likely will have adequate detail to specify the ISAPs at the outset of your planning phase. There are numerous security areas to be considered that should be delineated as part of your assessment process. However, to give you a jump start, we've included a list developed by the International Engineering Consortium (IEC) that delineates many of the major areas to be addressed in a comprehensive security project plan. Table 9.1 provides a list to help you to start thinking about what your network includes, what your security assessment should review, and what ISAPs you may need to define.

Remember, smaller projects are more successful, so if you need or want to undertake many (or all) of the items listed in Table 9.1, you should create separate ISAPs for them and roll them up into your corporate IT security project plan. At that point, the corporate IT security project plan becomes more of a "program" than a project, because it is the roll up of a number of related initiatives. This distinction is important, because looking at the corporate IT security project as a program allows you to allocate resources (time, money, expertise) across your IT security projects in a thoughtful and predictable manner, rather than running wild through one enormous project plan that is difficult (impossible) to effectively manage.

Table 9.1 Enterprise-wide Technology List for Security Projects

Technology Category	Components
Storage and Server Technology	Backup Solutions Disaster Recovery/Business Continuity Storage Management Solutions Story Area Network (SAN)/Network Attached Storage (NAS) Storage Server Provider (SSP) PCs/Workstations/Laptops Server Server-based Operating Systems

Continued

Table 9.1 continued Enterprise-wide Technology List for Security Projects

Technology Category	Components
Mobile and Wireless Technology	Wireless/Cellular Services Personal Area Networks (PANs) Wireless Local Area Networks (LANs) Fixed-Access/Point-to-Point/MAN Wireless Wide Area Networks (WANs) Mobile Computing Platforms/Applications
Networking and Systems Management	Network/Application Monitoring/Performance Management Policy Management Traffic Management Management Service Provider (MSP) Web Monitoring Services
Security	Anti-Virus Software Virtual Private Network (VPN)/Firewalls Public Key Infrastructure (PKI) Authentication/Access Technology Intrusion Detection Systems (IDS) Encryption VPN/Security Services Certificate Authorities Security Management
Infrastructure	KVM Directory Services LAN Infrastructure WAN/MAN Infrastructure Service Provider/Carrier Class Equipment Remote Access Servers Printers UPS Caching and Load Balancing Collocation Services Internet Service Provider (ISP)

Continued

Table 9.1 continued Enterprise-wide Technology List for Security Projects

Technology Category	Components
	Carrier/Competitive Local Exchange Carrier (CLEC) Services
Digital Convergence	VoIP Videoconferencing Private Branch Exchange (PBX) Streaming Media Technology Web-enabled Call Centers Content Delivery Network (CDN) Services Unified Messaging
Business Applications	Application Servers Database Servers Web Servers E-Commerce Enterprise Resource Planning (ERP) CRM Enterprise Application Integration (EAI) Content Management Data Warehousing Business Intelligence Tools Development Tools

Once you've developed your high-level (and perhaps mid-level) WBS tasks, you can continue developing additional underlying detail as you would any WBS development process. Don't worry about defining the tasks in the correct order. The order in which tasks should be done will be determined later when you're creating your project schedule. The tasks will be undertaken based on dependencies, constraints, and available resources, so spending a lot of time ordering tasks at this point is usually unproductive. That said, there is usually a linear order in which we think about tasks; if keeping them in some semblance of order helps ensure you don't overlook any major or minor tasks, that's fine. Numbering the tasks at this point will help you keep track of them. If desired, you can re-number your tasks when you believe you have your final WBS, but don't expect numbers tasks to be performed sequentially once your project gets underway.

Project Risks

Identifying risks to the corporate IT security project plan is ideally a team effort. Everyone comes to a project with a distinct set of skills and a unique perspective. These are valuable assets in your risk identification, evaluation, and mitigation planning process. The objective of this phase of project planning is to identify all the things that could go wrong with your project and come up with specific plans for avoiding or reducing those risks.

There are three basic ways to deal with any risk. You can mitigate, avoid, or transfer. Let's look at a quick example to help illustrate these differentiations so you know how to approach project risk management.

- **Mitigation** If there is a fire danger, you buy fire sprinklers to reduce your risk of fire.
- **Avoidance** If there is a fire danger, you remove flammables from the area to avoid the risk.
- **Transference** If there is a fire danger, you buy fire insurance to make the risk someone else's.

Eight distinct steps should be taken in your risk management planning phase:

1. Identify the risk.
2. Rank the likelihood of the risk occurring.
3. Rank the severity of the impact should the risk occur.
4. Create a prioritized list of risks you will plan for and manage.
5. Develop mitigation strategies to avoid or reduce the impact of the risk.

6. Develop specific triggers for the risk mitigation (or alternative) strategy.
7. Analyze the potential impact of implementing the alternate strategy.
8. Identify any direct, indirect, and unintentional consequences of implementing the alternative strategy.

Not all risks are worth planning for, because they are either unlikely to occur or because the impact if they do occur is negligible. An asteroid hitting Earth would have a huge impact, but it's not worth planning for because the likelihood of that occurring is so small. But what about something less dramatic, such as your company's acquisition of another company? How likely is that to occur and how would it impact your corporate IT security project plan? In your case the answer might be that it is highly likely to occur and would have a major impact. What about a dramatic downturn in sales? How likely is that to occur in your business, industry or sector? If that were to occur, how would that impact your corporate IT security plan? You might decide that it's highly unlikely to occur, but it would have a major impact on your plan (because your IT budget would be slashed accordingly). What about the introduction of a new security technology? Would that impact your corporate IT security plan? It might if your security strategy involves staying on the leading edge of security and technology. How likely is that to occur? It depends largely on what technology you're talking about, but let's assume for this example that it's not very likely to occur but would have a huge impact if it did occur.

These are all high-level risks that may be appropriate because we're focusing on the corporate IT security plan, not the ISAPs. However, there may be additional risks you and your team identify that you want to address. This is where an all-out brainstorming session can be very helpful. Have everyone identify absolutely every risk you can think of, whether they're realistic, outlandish, or highly unlikely to occur. Then have the team rank each potential risk twice (independently)—once for likelihood of occurrence and once for severity of occurrence. Place the list in prioritized order and review it. Sometimes a purely mathematical ordering of a risk's likelihood and severity doesn't address contextual issues very well; a bit of human intelligence can go a long way in developing your final list. Once you've accomplished this, decide how far down the list you're willing to plan. Develop risk mitigation strategies (covered that in detail in Chapter 6) appropriate to the plan and incorporate them into your project.

Project Constraints

As you know, every project has constraints that you must deal with. It's one of the major responsibilities of the IT project manager, and is what makes the job both challenging and interesting. Your corporate IT security project plan will undoubtedly have time, budget, and resource constraints you'll have to deal with. In addition, you will likely have legal or regulatory constraints that come into play. These need to be identified at the outset of your project.

In addition, you need to look at your project's scope, budget, schedule, and quality requirements and rank them from highest to lowest priority. Put another way, you need to understand which parameters are locked in and which are flexible. It's nearly impossible to demand that scope, time, budget, and quality all be etched in stone from the outset of the project, so you're better off defining which parameters can change and which cannot.

In the case of corporate IT security, you may find that your constraints are a compilation of the underlying ISAP plans, or you may find that your high-level constraints drive your ISAP constraints. There is no one right way to approach this, but it is important that you address it early and get project sponsor agreement as to project priorities. If you're operating under the assumption that budget is the top priority and your project sponsor believes you're working to come in on schedule knowing the budget may expand a bit, you have a potentially serious disconnect. Define these at the top level for your corporate IT security project based on your stated security strategy and alignment with corporate objectives.

This should give you a bit more flexibility in defining your constraints at the corporate IT security plan level and provide guidance as to how to proceed with the ISAPs.

Project Assumptions

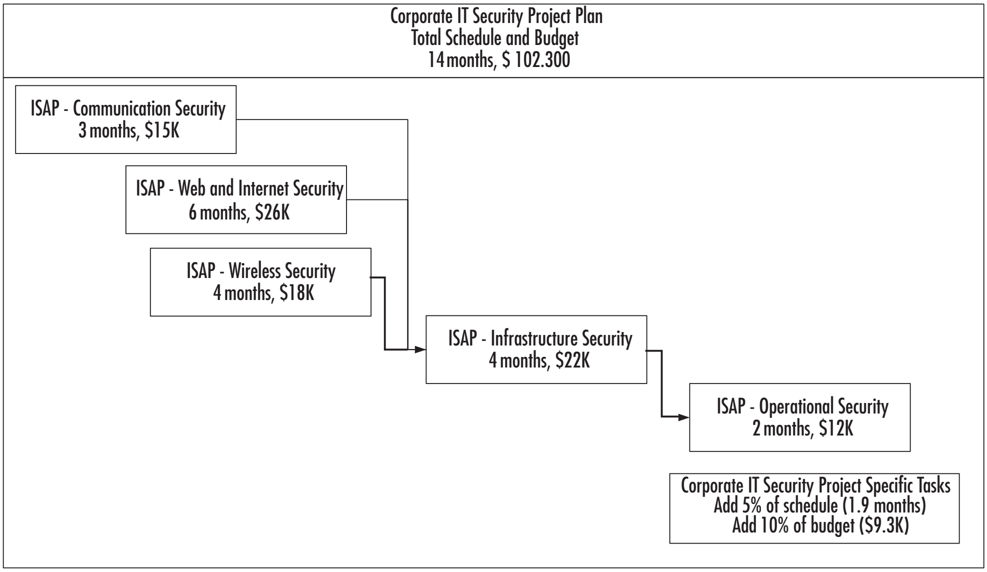
In order to undertake any project, you have to make a few assumptions such as that funding will be available or that resources will be released to you. The key here is to identify the assumptions you are making so that you can address them directly. If your corporate IT security project plan assumes the existence of an overarching security strategy, say so. If the strategy doesn't yet exist, then that assumption means you have some foundational work to do before you can implement your corporate IT security project plan. If you assume that your IT budget will remain a flat 5 percent of corporate revenue next year, state what dollar amount you believe that to be. When you list your assumptions, two things happen. First, you define what you're counting on as being true. Second, you're forced to look clearly at your project and think through what it is you are assuming. That's not always an easy process, because our assumptions sometimes are so fundamental that we can't see them clearly. Again, having your project team work with you on this will help avoid blind spots and make sure you clearly list the assumptions upon which this project is built.

Project Schedule and Budget

In terms of developing your corporate IT security project schedule and budget, there is one important note. If you approach it as you do any other IT project, you'll develop your schedule based on the logical order in which tasks should be performed, including the dependencies and the constraints. Your budget will be based on the calculated cost of each of the tasks and sub-tasks defined in the plan. However, there is one element to the corporate IT security planning process that is unique with regard to schedule and budget. You may choose to take a top-down or a bottom-up approach to your plan development. That is, you may choose to develop the various ISAPs and pull them altogether (with additional tasks that glue the corporate IT security project together and ensure a holistic approach) to create your project plan. This bottom-up approach means that your schedule and budget will also be built from the bottom up. Your schedule will look something like that shown in Figure 9.2, where your corporate plan is roughly the sum of the underlying ISAPs (there may be additional schedule and budget components for those "glue" tasks). In Figure 9.2, those "glue" tasks are shown as having no dependencies and 100 percent float, which is probably not how they'd be included in your project plan. They are shown in this manner to indicate there are tasks that are needed to tie these ISAPs together, such as a full systems test after all the ISAPs are complete or a complete review of all policies related to the ISAPs. The intent of the diagram is to show that the ISAPs roll up and essentially define the corporate IT security project schedule and budget.

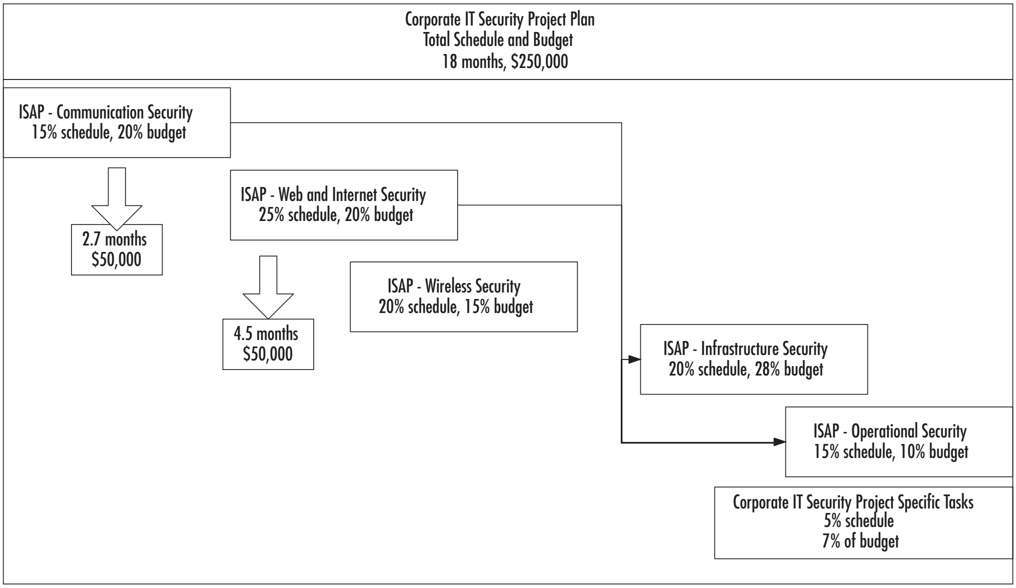
Notice that in Figure 9.2, there is overlap of some of the ISAPs. This might occur if you have enough IT staff time, resources, and expertise to undertake projects in parallel (e.g., you might use completely different staff to implement your Web and Internet security plan versus your wireless security plan). Based on other projects and workload, you determine if you can run these projects almost in parallel and that the first of those two can start when the communication security project is about 50 percent complete. Therefore, your total duration for your project is not the sum of the duration for each ISAP, but rather the total duration for all ISAPs to be completed.

Figure 9.2 Bottom-up Schedule and Budget Development


Corporate IT Security Project Plan
Total Schedule and Budget
14months, $ 102.300
ISAP - Communication Security
3 months, $15K
ISAP - Web and Internet Security
6 months, $26K
ISAP - Wireless Security
4 months, $18K
ISAP - Infrastructure Security
4 months, $22K
ISAP - Operational Security
2 months, $12K
Corporate IT Security Project Specific Tasks
Add 5% of schedule (1.9 months)
Add 10% of budget ($9.3K)

Alternately, you can define your schedule and your budget from the top-down, as shown in Figure 9.3. In this case, your total budget and schedule are defined and each ISAP underneath (as well as any "glue" tasks) are parsed out of the total. In this example, the total schedule allotted for your corporate IT security project plan is 18 months and your budget is $250,000. All of the ISAPs underneath are allocated a percentage or portion of the total. This may mean you have to scale time and budgets for the ISAPs down in order to meet your schedule and budget requirements, but you'd have to do that with either the approach anyway, since we're assuming you don't have unlimited time and unlimited funds to accomplish your goals.

Figure 9.3 Top-down Schedule and Budget Development


Corporate IT Security Project Plan
Total Schedule and Budget
18 months, $250,000
ISAP - Communication Security
15% schedule, 20% budget
2.7 months
$50,000
ISAP - Web and Internet Security
25% schedule, 20% budget
4.5 months
$50,000
ISAP - Wireless Security
20% schedule, 15% budget
ISAP - Infrastructure Security
20% schedule, 28% budget
ISAP - Operational Security
15% schedule, 10% budget
Corporate IT Security Project Specific Tasks
5% schedule
7% of budget

As with the bottom-up approach, some of your ISAPs may run in parallel or may begin before another project is complete. In the example shown in Figure 9.3, the wireless security plan begins when the Web and Internet project is about 50 percent complete, but that project can't commence until the communication plan is complete.

These examples are two ways you can incorporate your ISAPs into your corporate IT project plan and come up with a fairly accurate initial estimate for schedule and budget. It will have to be revised a number of times based on additional detail that is developed through the project planning stages, but deciding on your high-level approach to developing your corporate IT security project plan schedule and budget will help get you started for your initial estimates. This also gives you the opportunity to look at and address known parameters, constraints, and assumptions.

Business Intelligence…

Project Estimating: Part Science, Part Art

Project estimating—whether for scope, budget or schedule—is part science and part art. The science involves taking a consistent and methodical approach toward defining your tasks. The more detailed your WBS, the easier it becomes to define a unit of work (task) that can be clearly defined in terms of duration, effort, and cost. At the outset of project planning, you don't have that level of detail, but are often required to drawn a line in the sand and commit to the maximum cost and time the project will take. Dangerous waters, to be sure, but something we have to do almost daily. The process of defining the project schedule and cost can be termed *progressive elaboration* where you progressively gather more detail as you move through your project planning phases. The art form comes from understanding how to generate that initial estimate, how to manage expectations, and how to estimate various unknowns. As you become more experienced in project management and estimating, you should find that your estimates are closer to reality than fiction. That's the fine art of estimating.

Managing the Project

We're assuming that your corporate IT security project is a series of ISAPs and that you will manage them accordingly. You will have the additional burden of balancing conflicting demands for resources and addressing the impact of one ISAP on another. There is no cookie cutter approach that will work in all circumstances. Program management is outside the scope of this book, but suffice it to say that it will test your skills as a project manager.

Closing Out the Project

Any project close out includes standard steps (see Chapter 8), but closing out the corporate IT security project plan also includes a number of elements unique to this type of project. It's entirely possible that you want to perform another security test or audit once all work is completed before officially closing out the project. This is one last check before you close the books on this project, and hand off the management of security for day-to-day management by your IT staff. Along the way, you should have developed processes and procedures for maintaining security on an ongoing basis; developed user training and guidelines, and developed an updated set of documentation for your IT staff to review, modify, and update on an ongoing basis.

There may be particular tasks or duties that need to transition out of the project mode and into the maintenance mode. Ongoing operations should support, sustain, or even improve the security set through the project activities. Documents, processes, and procedures should be reviewed and finalized for the operational team.

As with other important projects, your high-level corporate IT security project plan may also require a large presentation to executives or other key staff. Don't miss this chance to tout your team's efforts and project results. Highlight the positive, calmly explain the negative, and if necessary, explain what you've learned and how it will benefit the company in the future.

Summary

We've covered a tremendous amount of territory in this chapter, with the intent of helping you define your corporate IT security project plan based on the specific needs of your organization. Your corporate IT security plan should start with a well-defined enterprise-wide security strategy. This is the glue that binds all of your security activities together and provides the rationale for all IT security activities. Ideally, this is developed prior to trying to plan your corporate IT security plan, but in some cases, it might make sense to list it as the first major objective in your plan.

We took a look at various legal standards related to your corporate IT security plan, because in this day and age, security has become a legal issue. While this chapter won't make you an attorney, it should have provided enough of an overview to help you understand the larger legal environment. Of course, you should consult your firm's legal counsel for additional information on the potential legal implications of security in your particular company.

The bulk of this chapter walked you through the standard project management steps with an eye toward corporate IT security project planning. While the generally accepted project management methods apply in this case, there are areas specific to corporate IT security planning that we called out along the way. These are typically high-level issues that should be addressed in a top-level project plan. We also noted areas where the corporate IT project plan provides the mortar or glue for the ISAPs. Each individual plan should be complete unto itself, but there are necessary connections between and among the ISAPs required to implement a comprehensive, holistic IT security solution for your company.

At the end of all of this, you should have a fairly clear view into how to approach your unique corporate IT security project plan. Every company and every IT security solution has standard components as well as very distinct organizational requirements. Your challenge is to apply standardize methodologies while addressing the aspects unique to your company and your IT environment. This chapter provided the foundation upon which to build your corporate IT security project plan.

Solutions Fast Track

Defining Your Security Strategy

☑ Your IT security strategy should be aligned with the business objectives of your organization.

☑ IT security strategies developed without aligning with business objectives are far less likely to benefit from executive support or to receive needed funding.

☑ The five key success factors for an IT security strategy are: 1) The skills, capabilities, and efforts of the entire organization must be utilized and mobilized, 2) Key functions and processes in the organization must collaborate on shared security goals and strategy, 3) The organization's security objectives or an articulation of its "desired state" must be developed and understood, 4) Critical assets that are essential to achieving the organization's mission must be identified and protected, and 5) IT operations and support must enable security goals.

☑ Your corporate IT security plans also have to align with the reality of your organization. You must live within the company's constraints, which may include budget, schedule, staffing, or other overarching organizational limitations.

Legal Standards Relevant to Corporate IT Security

☑ There are numerous federal laws that impact corporate IT security. Some of the more well-known ones include: GLBA, HIPAA, SOX, FISMA, FERPA, TEACH, ECPA, and CFAA.

- ☑ There are numerous state laws that pertain to corporate IT security that you should be familiar with, especially with regard to all states in which your company has a physical presence.
- ☑ There are three key fallacies that can trap corporate and IT staff when planning for IT security: The "Single Law" fallacy, the "Private Entity" fallacy, and the "Penetration Test Only" fallacy.
- ☑ There are a number of things you can do to reduce your company's legal liability including: Understand your legal environment, perform comprehensive and ongoing security assessments, evaluations, and implementations, use contracts to define rights and protect information, and use qualified third-party professionals.
- ☑ Nothing in this chapter or book should be construed as legal information or advice. You should consult with a qualified legal professional to assess your firm's specific legal liabilities and to develop optimal legal risk mitigation strategies.

Corporate IT Security Project Plan Overview

- ☑ Your corporate IT security project should be based on your overall security strategy for the organization.
- ☑ As with any project, you should define the problem you're trying to solve so your project solves the right problem.
- ☑ An integral part of the problem definition in IT security is the security assessment or audit.
- ☑ You may choose to perform the assessment as a separate project or as the first major task in your corporate IT security project plan.
- ☑ The remaining steps mirror standard project management steps: Define the desired (required) outcome(s), identify potential solutions, define project constraints, define project requirements, select optimal solution, define project team, define project

procedures, define project WBS, tasks, owners, resources, budget and schedule, monitor and manage project, and hand off and close out project.

Corporate Security Auditing

☑ Security assessments and auditing are a natural first step for any IT security project.Your corporate IT security project may have such an assessment as the first major objective or you may develop your plan based on the outcome of a separate security assessment project.

☑ Security fails for a variety of reasons, the primary reasons being: Improper configuration, failure to update, faulty requirements, human factors, policy issues, and incorrect assumptions.

Corporate Security Project Parameters

☑ Your corporate IT security plan should start with defining the key objectives.

☑ Every project includes four parameters that must be balanced: scope, cost (budget), time (schedule), and quality.

☑ There are numerous skills needed for each IT security project. These generally can be organized into these categories: Operating system skills, network skills, application skills, security tools skills, programming skills, compiled languages and programming skills, and scripting languages.

☑ As part of the initial project definition, you will also need to identify the key personnel needed.

☑ Defining project processes and procedures is an important part of any IT project, but in the corporate IT security project plan, you need to define enterprise-wide processes to address the unique characteristics of this type of plan.

Project WBS

☑ Creating a WBS for your corporate IT security project may involve developing high-level tasks that include development of ISAPs as single task, or you may develop a WBS that pulls of the ISAPs in as separate project plans.

☑ There are numerous areas that must be addressed in the corporate IT security project plan including people, process, and technology.

☑ The WBS should include all subtasks and should be an iterative process to produce ever expanding levels of detail.

Project Risks

☑ Defining project risks and mitigation strategies is a fairly standard process, but at the corporate IT security project level, there are organizational issues that must be addressed.

☑ One risk unique to the corporate IT security strategy that you might not find in other types of IT projects is the legal risk.

Project Constraints

☑ If your corporate IT security project plan is well-aligned to your current business strategies, you should be able to identify your project constraints in a manner consistent with organizational goals.

☑ Understanding at a corporate level how scope, budget, schedule, and quality all come into play and what the priorities should be for both the corporate IT security project plan and the ISAPs, will help you manage the program (collection of related projects).

Project Assumptions

☑ Many of your project assumptions will be related to the underlying ISAPs, but they can also be captured in the corporate IT security project plan.

☑ Your high-level assumptions about your business environment are assumptions that should be captured in your plan. These may include assumptions about your overall level of funding in the coming year, planned acquisitions or divestitures, and so on.

Project Schedule and Budget

☑ When creating your corporate IT security project plan, your initial schedule and budget estimates can be developed using a bottom-up or top-down approach.

☑ A bottom-up approach allows you to create your best estimates for the underlying ISAPs, add some factor for the corporate IT security project-specific activities, and develop a top-level project schedule and budget.

☑ A top-down approach allows you to determine the total time and budget for all corporate IT security projects, and allocate time and dollars as percentages of the whole. This might be desirable if you have very specific deadlines and budgetary targets you're trying to meet.

☑ Running the corporate IT security project is like managing a program because you'll have to deal with potentially conflicting needs of the various ISAPs as well as corporate constraints.

☑ Closing out the project should include transitioning needed ongoing security activities to the daily operational staff. Documentation should be reviewed, revised, and finalized to provide the procedures, policies, and documentation needed to support, sustain, and improve security in the future.