Chapter 6

Planning The IT Security Project

Solutions in this chapter:

- **Creating the IT Security Project Work Breakdown Structure**
- **Defining Project Tasks and Sub-tasks**
- **Checking Project Scope**
- **Developing Task Details**
- **Identifying and Working With the Critical Path**
- **Testing IT Security Project Results**
- **Budget, Schedule, Risks, and Communications**

☑ **Summary**

☑ **Solutions Fast Track**

Introduction

We've arrived at what many consider the heart of the project management planning stage. Each of the other activities described in earlier chapters of this book is vital to the success of the project, but some of what is required in those other steps can't be fully completed until the work described in this chapter is complete. Once you complete this chapter, you should go back and review the first five chapters to revisit and revise your data.

In this chapter, we define the specific tasks that make up the project work package or "deliverables." Keep in mind that we're discussing two different project types in this book: the overarching master security project plan, and the smaller, individual security area project plans. Together, you have a total security project plan that incorporates the specific security elements relevant to your company. In later chapters, we show you Work Breakdown Structures (WBS) for various individual security area project plans. If you're familiar with WBS, this chapter provides details related to security that will be helpful to you. If you're a bit rusty on your project management skills, this chapter will also provide a quick refresher.

Creating the IT Security Project Work Breakdown Structure

The WBS is like a "to do" list only with more muscle. It is a list of all the major and minor tasks that need to be accomplished in a project. It is most easily created by starting with the three to five project objectives you created in Chapter 3. Those three to five major objectives can each be broken down into major tasks that, when completed, would achieve that particular objective. Be sure that your WBS tasks are at the same level. Many people have a tendency to dig down into the detail on some tasks, but not on others, so keep this in mind. Some people find it helpful to use a standard outline form to ensure their WBS makes sense. For example, suppose your project was to secure your home wireless network. The major steps would be:

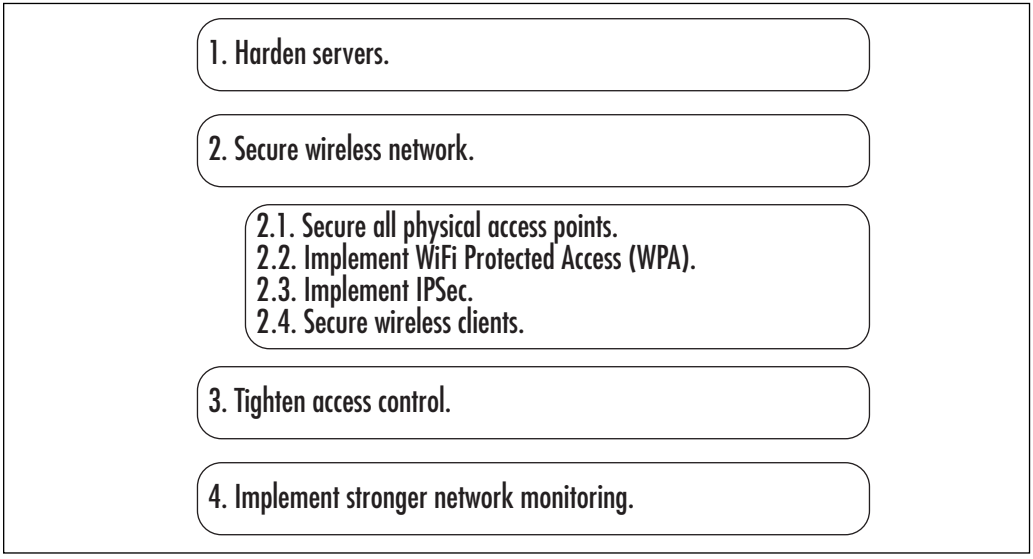
1. Configure what router to use unique to Service Set Identifier (SSID).
   1.1 Log into the Wireless Application Protocol (WAP) or router administrator account.
   1.2 Locate the access point name and modify the default name to a unique name.
   1.3 Locate the SSID and change the default name to a unique name.
   1.4 Log out of the WAP or router administrator account.
2. Disable the SSID broadcast.
3. Enable security (Wireless Encryption Protocol [WEP] or Wi-Fi Protected Access [WPA]).
4. Configure Media Access Control (MAC) address filtering.

If 1.1, 1.2, 1.3, or 1.4 were at the same level as 2, 3 or 4, you would not have good construction (e.g., because 1c is at a deeper level of detail than items 2 or 3). By using this outline form, you can insert detail as you think of it, while keeping track of the levels. There are many different ways people create the WBS. Some advocate simply listing out all the tasks you can possibly think of and ordering them later. However, most people think through tasks in a fairly linear way, so creating an outline and then popping in details that may come to mind out of order is also an acceptable way of approaching the WBS.

The key is not to get sidetracked by trying to place your tasks in order at the same time you're thinking of them. If you're working on this with your initial project team (a recommended approach), you should try to use a white board and simply list all the tasks you can collectively think of and then organize them. If you do it this way, you will find that tasks at all levels of the WBS pop out in random order, and that's fine. Capture them and order them later. If you try to approach this too methodically, you're likely to overlook or omit something, because you'll be too busy trying to keep everything in order rather than making sure you're covering all your bases.

A sample security WBS for an Information Technology (IT) security project plan might look something like that shown in Figure 6.1. Notice that we've stayed at a fairly high level at this point. We're assuming we've already audited network security and identified security needs, though these can be part of a master security project plan. (Chapter 10 walks you through a security assessment and auditing project plan.) We've got a bit of detail under task 2, but we've indented those subtasks and used a sub-numbering system to indicate the relationship of those tasks to the top-level task. Later, we can refer just to task 2.4 or 2.4.1 (a subtask of that task), and readily understand the relationship among these tasks. In later chapters, we walk through more specific WBS structures for Individual Security Area Projects (ISAPs). The structure shown in Figure 6.1 is not the only structure your WBS can take, but it is commonly used and is probably familiar to you.

Figure 6.1 Sample WBS (Top Level)



In any security-related project, there's a good chance you'll find tasks that span the boundaries between two different projects. We've talked

about the corporate IT security project as separate from the individual security area projects (ISAPs), but in reality, there are all interrelated. When you're creating your security project plan, you're well aware of the fact that you can't look at security in silos. What you do in one area often impacts another, which is why we describe the corporate IT security project plan as the glue that binds the ISAPs together, and ensures you have a comprehensive approach to security. As you develop your WBS for any security-related project, be sure to capture tasks that either fall completely outside the scope of your project, or that span the boundaries. You can capture them as un-numbered tasks, or you can place them in a "parking lot" file. Just be sure to capture them, and make sure they're addressed at some point.

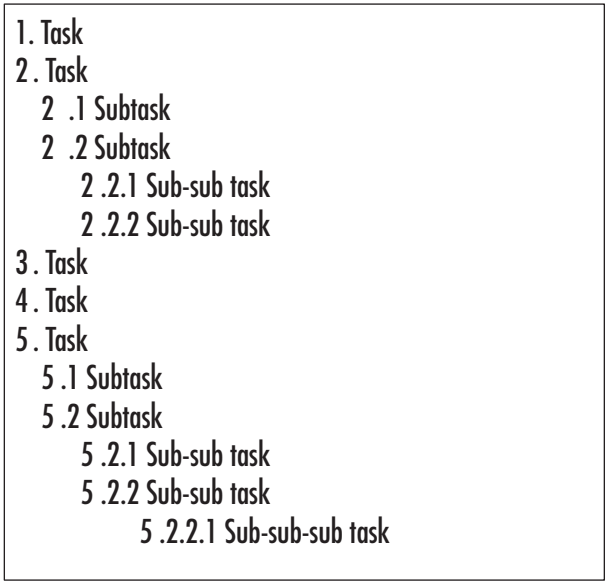
Defining Project Tasks and Sub-tasks

As shown in Figure 6.1, Task 2 has four sub-tasks defined. Typically, you would define the major tasks and go back and identify the sub-tasks (in this case 2.1, 2.2, and so forth) afterward. For each major task, you will then develop sub-tasks. Some IT project managers find it helpful to assign each major task to a subset of the project team and have them work through the details. For example, you might have your wireless experts develop the tasks for Task 2, so that they bring their expertise to bear on the development of those related tasks. Who better to recommend tasks for securing your wireless network than your wireless experts? While it may sound obvious, you'd be surprised how many times in the frenzy of planning a project that these things get overlooked. While planning is almost always improved by the input of subject matter experts, it is doubly so with IT security. An error or omission in security can mean you've left the door open for the bad guys.

Though we're assuming you have strong project management skills, a quick refresher never hurts. Keep these things in mind while you create your WBS:

1. Don't worry about the order in which you define your tasks (or sub-tasks). You can reorder them later.
2. Tasks should use a verb/noun format. Avoid using "Access control" as a task name. Instead, use "Tighten access control" or "Test access control" so the intent of the task is clear.
3. Use a numbering system that makes sense to you. One commonly used one is shown in Figure 6.2.
4. You can go down any number of levels, depending on the level of detail you want to define for each task. There is a point of diminishing returns, so define a reasonable amount of detail. Additional detail can be defined and captured in the task's details.
5. Once you believe your WBS is complete, review it thoroughly when you're alert, refreshed, and focused. Have your security project plan team review it for errors or gaps, as well.

Figure 6.2 Sample Work Breakdown Numbering System



Checking Project Scope

Once you've identified your project's tasks, sub-tasks, and so on, you should have a very clear idea of what the project looks like. If not, you need to do more work on defining your tasks. If your task list is a thousand miles long and filled with tasks like, "Sharpen all red pencils," your task list is too detailed and you need to scale it back a bit. Then, look at all the tasks and see if they fit within your defined project scope. This is your first real opportunity to do a "scope check" and ensure that all the work you've defined fits within your stated scope. More often than not, a good WBS will detail more work than was included in the initial scope. That's natural, because we tend to be able to better define the project the further into it we get. However, the problem it creates is rather obvious—you have approval to do "X" amount of work and your project plan has delineated "2X" work.

You have several choices at this point, but the most obvious are to either scale back your WBS or increase your scope. Now for your spot quiz: If you increase the scope of your project, what else must change? If you answered time, budget, or quality, then you know your project management well. If you increase your scope at this point, you'll have to renegotiate the amount of time you'll have to complete the project (more), the amount of money you'll need to complete the project (more), or the quality (less) you'll be able to deliver if time and cost cannot change.

Your second choice is to look at your security project plan and your WBS and decide if there are any elements that are not crucial to the successful completion of the project. Sometimes when people get into WBS mode, they start defining their "wish list," or they include everything they can think of. Sometimes this can be an effective way to accomplish things in the organization that has been looking for a project, but most of the time it just clouds the issue. Clean out your WBS if you can't change your scope, time, schedule, or budget. Pare it down to the bare minimum and re-check your scope.

IT security projects are tricky to the extent that if your WBS defines a scope of work that is larger than the initial discussion or agreement about the scope, you need to really ask yourself what should "give." Should it be the scope or some of the tasks in the WBS? How can you decide when you're talking about network security? While our tendency is usually to say "It's all important!" the truth is that if you carefully review your WBS, you may actually find tasks that can either be put into a different security project plan or that may truly be redundant or optional. Finally, this situation may force you and your team to get a bit creative and think of ways you can scale things back and actually improve your security or your security project plan (or both). The old expression "Necessity is the mother of invention" sometimes holds true, and if you and your team put your collective minds to it, you may be able to find ways to increase security while scaling back the project scope.

This is also a great time to check in with your security project plan sponsor. Run the WBS by him or her and gain approval for your WBS and your scope. If there are problems, now is the time to find them and fix them. If you find yourself in the position of having to go to bat for a larger budget or longer schedule, you should be prepared to make the business case for this. Remember, it's natural that you would have a better idea of the project's scope once you've created your WBS, because the act of creating the WBS drives clarity. With that clarity should come an understanding of the areas in which the project has grown. If you believe these are important areas to include, then clearly link each of these areas to the business objectives, the risks of not addressing these areas, and potential alternatives to addressing these areas (e.g., you might prioritize several of the items and agree to make them part of a Phase II project, because you and your team believe that, while important, these items may not be pressing or critical in the near-term). Finding creative solutions and bringing alternatives to the table is always preferable to saying, in essence, "We need a bigger budget. Period." Sometimes that works, especially if the items are critical areas to address, but often the answer is, "Find something else to cut out of it then." It may be a negotiation, but if your network security is at risk, it's worth putting some effort into dis-

covering ways to get it done. If you need some fuel for your fire, check out Chapter 9 where we discuss some of the legal ramifications of not securing your network. Better yet, do a bit of Internet research and look for recent articles pointing out the cost or ramifications of a security breach. If you can find a company like yours or in the same kind of business, it might really drive the point home. There's nothing like a little reality check from time to time.

Business Intelligence…

Smaller is Better When it Comes to Scope

As we discussed in Chapter 1, studies have consistently shown that smaller projects are more successful. That makes sense when you think about it; it's easier to get your arms wrapped around a project, it's easier to keep staff motivated and focused, it's easier to monitor progress, and so on. One of the first places you'll begin to get a sense of the scope of your project is once you've made the first or second pass through your WBS. As you define the tasks and sub-tasks, you'll see the scope of the project more clearly. Sometimes in the process of delineating your WBS, you see that your scope has expanded significantly. Other times, your WBS may indicate the project isn't as large and complex as you'd first thought (a somewhat rare occurrence). Using your WBS to gauge your scope can help you decide whether you need to break your project down into smaller projects, or whether your scope managed to creep up during the definition phase of the project lifecycle. Whatever the case, your WBS will define your scope, and this is an excellent time to check your scope and make the necessary adjustments. If the scope is out of control at this point, your project is not likely to succeed.

Developing Task Details

There are numerous *task details* you can include in your IT security project plan, but we're going to focus on two types of details—the most commonly used task details and the details that specifically relate to IT

security. We're taking a two-pronged approach, because people often skip over defining even basic task details, and these details (both basic and security-related) are extremely helpful project management tools.

How you develop your task details is somewhat a matter of personal project management style, but there are some guidelines that will help you develop really solid task details. First, the person or group that will be performing the task is typically the best resource for helping to define task details. To go back to our wireless example, you're better off having your wireless expert define the wireless security task details, than having your database administrator define them. The experts can usually define the task detail more quickly and effectively than the project manager can; therefore, rather than sitting down one late night and trying to define all these task details, begin delegating at this point. It's an obvious but sometimes overlooked piece of the puzzle.

Owner

The first task detail that comes to mind is the *task owner*. In an IT security project, you may choose to have security area experts head up the ISAPs; therefore, they may be considered the owners for tasks related to his or her individual security area. You may choose to assign ownership of tasks to those who will oversee the work or to those who will actually do the work. It depends largely on how your IT organization is structured. In any case, there is a rule about task ownership that you should heed: "A task with no owners won't get done; a task with two owners won't get done." In other words, a task should have only one owner. That owner may or may not complete the work itself, but he or she is responsible for the work getting done. If you have two or more task owners, no one takes responsibility for the task, and you, as the IT project manager, won't know who to hold accountable (e.g., Jose says it was Keiko's responsibility; Keiko says she thought Manish had it under control; Manish says he thought Larry was heading it up; and Larry says he thought Jose said (in a meeting last week) that he had completed the task. Assign one owner per task to maintain accountability and responsibility for task completion.

Resources

The term *resources* can be used to indicate anything needed for a security project plan's completion, whether that's people, money, tools, equipment, software, or supplies. For each task, you should have the task owner (or a subject matter expert) define the resources needed for that task. While they may not know exactly which resources they need, they should define (at a minimum) the people or skills required and any known tools, software, or equipment they can think of. These two types of resources—people and supplies—are used both in scheduling and in budgeting, so defining these elements at this stage will be very helpful in developing your initial project schedule and budget. Remember, project management is an iterative process, so you'll probably have to go back to this a few times to hone the details as the picture becomes clearer.

With an IT security project, you're likely to need resources that you, as the project manager, may not know about or even understand. Do you know what AirSnort is, how it's used, or what it might cost? Would you think to include the cost or even require the use of these tools in your wireless security project plan? (Ironically, many hacker tools are available as standard tools built right into operating systems, or as free shareware programs widely available on the Internet). If you're a wireless security expert, you might. If you're an IT manager or an IT project manager that might not be your strength, therefore, relying on your subject matter experts to help define the needed resources for tasks is critical. Otherwise, you may lack the tools or expertise needed to secure your network, or you may find yourself at the short end of your budget quicker than anticipated.

Also, because IT security project plans require specific expertise in key areas, you should also require your subject matter experts to define the type of expertise required to perform a particular security task. If the task is to review Access Control Lists (ACLs) on several key network objects, anyone on your IT staff could probably complete that task. However, if the task is to test the database so that script errors won't provide an opening to hackers, there's a good chance you need a database expert to

help you with that. So, be sure to define required expertise within your task resources. This will help ensure you have the expertise needed for the task, and will also help you better estimate what skills and knowledge you'll need to complete your IT security project plan. That might mean training internal staff or contracting out, but you need to know this going into the project so that you can properly allocate time, money, and resources.

Completion Criteria

We briefly discussed *completion criteria* earlier, so we'll quickly revisit it here. Completion criteria are the criteria by which you or anyone else can determine if a task was completed properly. Completion criteria can be a simple checklist or a more comprehensive set of standards or protocols. Whatever will be used to determine if the task was successfully completed should be defined in advance, in the completion criteria for the task. Often, the task owner or the subject matter expert is the best person to create these completion criteria; however, sometimes additional research may be required. It's also possible that you won't be able to define the completion criteria for some of the tasks until later in the project cycle, when you have a better understanding of the project. Defining completion criteria for a security project is absolutely crucial. The number of errors and omissions drops significantly when you define the completion criteria for each task. In addition, when you define these criteria at the beginning of the security project plan lifecycle (when things are relatively calm), you reduce your chance of missing something important once the project is in full swing.

Also keep in mind that if you have specific requirements—whether functional, technical, legal, or regulatory—they should be addressed via the completion criteria in the tasks. Quality is built into a project through task details, and one of the most important task details are the completion criteria. If you need to meet specific requirements, build this into your task detail via the completion criteria, to ensure the requirements actually are met. Otherwise, it's a bit of a crap shoot.

Schedule

Best practices in project management include the use of the 8/80 rule when defining the *schedule*. This rule states that you should not define any task that takes less than 8 hours, and no single task should take more than 80 hours. This is a very broad guideline, but it helps on both ends of the scheduling spectrum. Obviously, if you schedule tasks that are less than 8 hours, you're headed for an absolute scheduling nightmare. On the other hand, if you have a task that takes more than 80 hours, there's a good chance it can be broken down into smaller tasks that are more manageable.

Once you've created your IT security project plan's WBS (for the corporate IT security project plan or any of the ISAPs), you can begin estimating task duration. Let's take a moment to distinguish between *duration* and *effort*. You're probably familiar with these two terms, but it's important to understand the difference. *Duration* is the amount of time you allot for the task to be completed. *Effort* is the actual amount of time it takes to complete the task (e.g., you may schedule two weeks (duration) to implement network server auditing, but the actual task of setting up that auditing might take a total of 4 hours (effort). Successful security project plans schedule around duration, not effort. Most of the people (probably all of them) on your project team have other duties, responsibilities, and deliverables. By scheduling the duration, you're defining in what time period the task needs to be completed. One person might complete the task on Day 1 of the two-week duration, another might not be able to complete it until Day 14. It's 4 hours worth of work that has to be scheduled in among other conflicting priorities. Using the duration will give your security project plan team members the flexibility needed to complete their tasks in a manner that fits their workload.

Once you've defined task duration, you can begin to get a sense of how long your project will take to complete. We haven't yet discussed dependencies, which can push your schedule out further, nor have we talked about scheduling resources, which can expand or contract your schedule, but duration will give you a high-level sense of your project's overall schedule length.

Budget

If you've defined all of your tasks and identified the needed resources, it stands to reason you should be able to develop your preliminary budget at this point, right? Well, yes and no. You can go through your tasks and identify the resources needed—both in terms of people and supplies—but that doesn't necessarily account for all of your IT security costs. It doesn't include training (e.g., hiring outside contractors to fill in for three team members that will be in China starting up a new corporate division for six weeks during your project). These are the kinds of things that can break a budget and they often sneak up on you. So, once you've defined your tasks, needed resources, and required expertise, you may want to get the team together to talk about what you might be missing from your budget. In an IT security project plan, you almost certainly will require tools, training, and equipment. Some of those resources will be specific to an ISAP, and others will be useful across several ISAPs or in your corporate IT security project plan. Look for areas where you can leverage resources to reduce the overall cost of your security project plan budget. When you can show executives they're getting more "bang for the buck"' with some of their IT security expenditures, they may be less reluctant to approve the purchase.

You may need assistance in creating a budget from your Finance department. If that type of resource is available, take advantage of it. Having someone well-versed in creating a line item budget can help speed the process and make sure you don't overlook important budget components.

Dependencies

If you've created even one project plan, you know that defining *dependencies* is a key task in your planning process, because it ultimately determines the length of your schedule. If you fail to identify dependencies, you will end up with excessive idle time in the project, or you'll end up crashing your schedule to get it completed in time. If your dependencies are linked to external events, you have additional challenges to consider.

In an IT security project, there are numerous interconnected elements that can impact your schedule that should be listed as dependencies. Hardening your servers may be dependent upon upgrading several of the operating systems or some other task. The order in which you perform these tasks may be vitally important, and identifying the dependencies properly, and therefore performing the tasks in the requisite order, can literally mean the difference between having or not having a secure network.

Different people use different methods of identifying and recording dependencies. Some people like to use sticky notes, placing them on a whiteboard, drawing lines to define dependencies, and then loading all of that data into a project management software program. Others prefer to identify dependencies within the project management software program right from the start. Your subject matter experts are a good source of data about dependencies, because they can tell you that if you do Task 7.2.3 before Task 4.1.9 you will generate errors and Task 3.3.5 will fail. Finally, if you are developing your dependencies for your ISAP, you should note all of the dependencies that link to or rely on external tasks, activities, or events. Be sure to mark these dependencies in the relevant tasks, and create milestones in your security project plan schedule to indicate the need to link to external data, tasks, or events.

Constraints

Constraints impact projects by limiting the approach or methods the team can use to complete the project. Constraints can be internal or external to your department, division, or company. What are the kinds of constraints you're likely to find in an IT security project plan? Some are the same as any other project, and some are unique to security. While your list of constraints might be longer, shorter, or contain different items, the following are five elements that are likely found on many lists:

1. Expertise
2. Tools
3. Budget
4. Organizational change
5. Governmental or regulatory requirements

Expertise

As mentioned earlier, the lack of specific security expertise is a constraint that should be carefully considered. If you lack the depth and breadth of expertise on a particular aspect of security that is vital to your security project plan, you will need to figure out the best way to address that gap. These constraints can cause difficulty in your project planning and execution, because, unlike standard IT projects, security project plans can be less forgiving (i.e., someone is often waiting for you to make a mistake so they can exploit it).

If you find your security project plan needs specific expertise, and if you believe this expertise is in short supply, difficult to locate, or very expensive, this is a significant constraint on your project that should be noted and addressed with your security project plan sponsor.

Tools

Sometimes tools can be a constraint, especially if one of your subject matter experts recommends (or requires) a particular tool and your budget can't accommodate it. If there's a piece of equipment that you share with another department, or a piece of equipment you need to rent or lease, list this as a constraint as well, since it could impact the ability of your project team to move on to specific tasks that require the use of this tool or equipment.

Budget

Is a *budget* ever large enough? Probably not, but in the world of IT security, a skimpy budget may translate into network vulnerability or, even

more importantly, legal liability. Don't let your corporate executives tell you to be "penny wise and pound foolish." You might be able to shave a few thousand dollars off the budget, but you need to assess the risks of doing so. If your budget has a bit of fat that can be trimmed, great. If not, then you're starting to cut into the muscle of your project and need to clearly delineate the risks to your boss, security project plan sponsor, or corporate executives.

Sometimes the issue isn't the total amount of money, but the timing of the funds (e.g., smaller companies often track [and manage] their cash flows very tightly). It's possible that your budget for this project was approved, but you're later told that you can't spend that $10,000 on x, y, or z until June, because the company doesn't have the cash. Clearly, this is a constraint that impacts your team's ability to get the security project plan completed on time; therefore, it should be listed as a constraint. If you're really on top of your game, you will prepare a cash flow model for your project so that you can define when you'll need which amounts of capital. If this is beyond your skill set, see if you can offer one of the Finance people a free lunch or a pair of movie tickets to help you project your cash expenditures during the lifecycle of the security project plan. Your executives will be impressed and your Finance folks will probably be relieved to have an idea of when these expenditures might come in.

Organizational Change

Sometimes *changes to the organization* can create project constraints that we don't immediately recognize. If your company is in the process of evaluating another company for acquisition, this might be a constraint on your security project. You might not be able to conclude your project in a timely manner if your project resources are reallocated to another project, or are unavailable due to this acquisition. While this scenario may not be relevant to your organization, take a look around your company and see if there are any upcoming changes that could constrain on your project.

Governmental or Regulatory Requirements

Governmental or regulatory requirements have an impact on an IT security project plan. Are these constraints? It depends on the nature of the requirements. In some cases, these might simply be included in the functional and technical requirements. In other cases, these regulations might be constraints on the project as a whole. Any governmental or regulatory requirement that limits the way your team approaches the project should be considered a constraint and should be listed.

Along with constraints, you may also want to make a note of how that constraint impacts your security project plan, the approach to your plan, or methods the plan can use. Typically, constraints are risks or challenges you must live with, but any planning you can do to mitigate these constraints is usually worth the effort.

Business Intelligence…

Compliance Confusion

The ever-changing landscape of compliance clearly impacts IT security project plans, especially in the planning stages. While you should certainly utilize standard IT project methodologies, you also have to implement whatever additional tools and techniques are needed to become or remain compliant. We've stressed the importance of involving executives and users throughout the process, because at the end of the day, you're only as secure or compliant as your users allow you to be. All the access controls in the world won't help when an authorized user prints out a patient's medical file for review and accidentally leaves it at a coffee shop after a hectic morning. We'll talk about security policies and procedures later in this book, but you may want to add some additional planning steps to your IT security project plan to ensure that your organization can become and remain compliant with whatever regulations apply to your firm. The document called "8 Steps to Compliance Readiness" on Gantthead.com is helpful, and can be found at www.gantthead.com/article.cfm?ID=228710.

Lessons Learned

You may want to define and capture *lessons learned* as tasks are being completed. It's very common for these key findings to get lost as people move onto new tasks or new projects. Trying to sit down at the end of a project and gather lessons learned is like sifting through sand; most of it falls through the cracks. Although a particular task may not lead to a major "a ha" moment, it could certainly lead to a new or refined best practice, or just a slight modification to a test procedure that lends itself to improved productivity, better security, or less user frustration. Whatever is learned, the task work should be captured as part of the task detail. As part of your project processes and procedures, you can convene a "lessons learned" meeting each month or each quarter and have everyone compile the lessons learned from their tasks. Discussing these frequently and regularly can save other IT security project plan team members time and effort on later tasks, it can streamline and improve your project, and it can help everyone avoid common pitfalls or share better methods. If you wait to gather these at the end of your project, you not only risk having these innovations be forgotten, but you miss the opportunity for team members to benefit from this knowledge earlier in the project lifecycle.

Identifying and Working With the Critical Path

Sometimes people use an incorrect definition for *critical path*; therefore, let's start by defining it so that we all start from the same baseline. By definition, the critical path is the longest, least flexible path through your project. If any task that is on the critical path slips (e.g., is late), the project will not be finished on time. Most project management software programs will graphically show you the critical path after you've loaded in your task dependencies and duration.

The critical take-away here is that you should be clear about which tasks are on your critical path and which are not, especially within your ISAPs. It will help you make better decisions about how to allocate

resources to your project. If one ISAP is delayed, it might ripple through your corporate IT security project plan and delay the start or completion of other ISAPs. Ultimately, this impacts your overall network security because the longer it takes you to complete various elements of your corporate IT security plan, the longer the bad guys have to work on weak targets.

Testing IT Security Project Results

How you approach testing your *security project plan results* and security is up to you. You may choose to develop a wholly independent testing plan. You may also choose to develop testing criteria within tasks or phases of your project. Because you're dealing with network security, it's important to decide how you will test project results before you launch into your project. If you choose to develop an independent testing plan, you should tie in key tests or test points to your task details (e.g., if a task is defined as "Harden Server 123," completion criteria should be localized tests on Server 123 to ensure the hardening tasks were successful). However, since Server 123 doesn't live in isolation, a more expansive test will also need to be performed to ensure that the cross-boundary issues are addressed (e.g., what protocols, applications, or users are connecting to Server 123, and are all of those areas secure as well.). If a user is accessing confidential data located on Server 123, and Server 123 is secure, that's great. But what about the fact that the user is in the Dallas airport using an unsecured wireless connection? Now how secure it that data? Even if the user is connecting to a secure Web site requiring a user login, that data is still traveling from the laptop through the unsecured wireless connection to a hardwired Internet connection before traveling on to the secure site. Since security is defined by the weakest link, this particular scenario describes a secure server and unsecured confidential data. Do your testing procedures for Server 123 account for this? Probably not, because it's outside the scope of the task, "Harden Server 123." Therefore, your project planning should include testing procedures that test down (ISAPs) and across (corporate) the enterprise. (Figure 7.1 represents the cross-

boundary issues.) However, be sure your security project plan includes testing procedures.

As a reminder, it's often helpful to look at testing in terms of *people*, *process*, and *technology*. The *people* aspect has to do with testing how people can (and do) interact with network resources. *Process* has to do with testing various security processes, whether through settings, automation, or interactive testing. *Technology* has to do with verifying configuration, hardware, and software settings. If you look at these three areas in your testing plan, you're more likely to develop a comprehensive test plan.

While you've probably looked at your enterprise and decided what's included, now's a good time to review your project and what it encompasses. Is there something you've thought of that you want to test that is *not* included in the project plan or the WBS? If so, this is a good indication that there is an omission that should be addressed. (For your review, we've included a list in Chapter 9 of potential areas that might need to be included in your security project plan or might need to be part of your test plan [see Table 9.1].). While this list is long, it is not exhaustive, and you should take a close look at your organization to see what else might need to be included.

Testing plans vary significantly from one type of project to another, but a common set of steps for testing include the:

1. Testing stage
2. Schedule of the test
3. Location of the test
4. Participants in the test
5. Environment; general IT and equipment
6. Data to be used for testing
7. Backup and restore procedures
8. Testing procedure
9. Issue, problem, and error reporting procedure
10. Issue resolution procedure

11. Retesting procedure
12. Signoff procedure

We've also included a list of test types that will provide a reminder as to how you want to develop your testing plans. These will be very specific to both your organization, the risks, the threats, and the types of technology you have (ISAPs), but here's a refresher to get you started:

1. Unit testing
2. Integration testing
3. Usability testing
4. Acceptance testing
5. Beta testing
6. Regression testing
7. Performance testing (stress and load testing, stability testing, and reliability testing)
8. Benchmark testing

Budget, Schedule, Risks, and Communications

Once you have the details generated via your WBS, you can create a more detailed budget and schedule. You can also step back and look at various project risks and develop mitigation strategies. Finally, you can develop your communication plans because you'll now have sufficient information to allow you to determine who needs to be in the loop with regard to your project.

Budget

If you're working on your corporate IT security plan, it will have to encompass the underlying budgets for all the ISAPs. If you don't have those project plans developed, be sure your budget contains placeholders

for those amounts. Also be sure to communicate this information to the appropriate parties. Clearly, you want to avoid a situation where the budget that is approved contains only a portion of your overall IT security project plan costs. You can create your high level corporate IT security project plan with ISAP budget placeholders, or you can delineate the cost of each ISAP and add to it the corporate IT security project plan piece. It's just two different approaches that will lead you to the same result. Either way, remember that your corporate IT security project budget is a sum of the underlying ISAP budgets and the costs of the discrete components of the corporate IT security project itself. When it comes to budget approval, you want to have all the projects included and not have to go back for a second round of budget approvals after your projects are underway.

Schedule

For the most part, the comments just made about the budget preparation hold true for the *schedule*, with a few minor exceptions. First, some portions of the project work can be run in parallel; therefore, the overall corporate IT security project plan schedule is not exactly the sum of all underlying schedules. However, as you look across your ISAPs and the corporate IT security project plan, you may discover scheduling conflicts that didn't come into play until you looked at all of the projects in a holistic manner. The scheduling component becomes more complex when you're juggling resources across multiple projects, so if you are tackling more than one ISAP project at a time (i.e., running in overlapping or parallel modes), you'll need to map out your resource requirements across all projects. This moves your corporate IT security project into the realm of *program* management. (A program is a collection of related projects.) If you need to schedule a number of projects, you will want to rely on a good project management software program to help you with resource load balancing.

Risks

Each project carries its own set of *risks*. As you know from your project management experience, the risks are both internal and external to the project. As with your budget and schedule, you have individual ISAP risks as well as risks to the overall corporate IT security project plan. It's possible that as you evaluate your projects, you'll see risks that span several ISAPs that were not present when looking at your projects one by one. One example of that kind of risk is that the resources you need won't be available at the right time. If several of your team members are working on one ISAP security project plan that gets delayed, it might have an impact on one or more of the other ISAPs. Looking holistically at your risks across the entire range of projects (ISAPs and corporate IT security project plan) will allow you to see the big picture and plan your risk mitigation strategies accordingly.

Communications

Communicating in the IT security project plan is really no different from other projects. It's included here because some IT project managers aren't great communicators, and this is a huge missed opportunity. An interesting statistic about security project plan success is that the *perception* of success is just as important as the actual results when people are asked to assess the project's success. So, you can knock yourself out to deliver the absolute best results only to find that, because you didn't do a good job communicating during the project, it's deemed "acceptable" at best.

Create communication plans and implement them. Remember the four C's: Communicate clearly, concisely, and consistently. Most people just want information, but many people in IT seem to think that if they don't know the answer, they should wait until they do know the answer before saying anything. Just the opposite is true. If you don't know, say you don't know, and then communicate what you're doing to find out when you'll next communicate. When you fail to communicate, your project falls into the corporate black hole and you lose the opportunity to maintain a positive attitude about the project and its results.

Business Intelligence…

Users Are the Key to Compliance and Security

IT security has become a major issue in the compliance arena, though that pointed focus is a bit misplaced. In some ways, IT security is the "low hanging fruit"—easy to point to and grab as the solution to this challenging problem. Computer and information technology is still an evolving field. Fifty years ago, no one had to worry about managing electronic information, so the answers we're seeking today have to be developed based on the ever-changing technological landscape. IT technologies must contribute to security, but in the end, people within the organization must be engaged in helping create and maintain security. There are different ways to do this, but continued visibility is an important aspect. Whether you have your Human Resources department or your Training department involved, be sure to consider creating a regular communication channel to educate and engage users in the security process. The Computer Security Institute has developed two regular newsletters, one focused on users and the other focused on top-level executives, that you can sign up to receive. They can be customized to your organization (i.e., you can add your logo, street address, and a small section for company-specific information) for regular distribution to your users and executives. This fee-based newsletter is just one solution, but it's a good idea to implement a system for keeping IT security and security practices in the forefront of your users' minds. You can take a look at sample newsletters at www.gocsi.com/awareness/publications.jhtml. Keeping users up-to-date about changing IT threats and security best practices is a great way to help bolster your IT security project plan results.

Summary

Planning an IT security project plan isn't dramatically different from planning any other kind of IT project, it just has a few nuances that are good to know about going in. We reviewed the basics of planning your IT security project plan and discussed those differences. The WBS is where the proverbial rubber hits the road, where the project details begin to take shape. Within your tasks, you can include the data that provides guidance on the successful completion of the tasks as it relates to your security requirements. Functional and technical requirements should be translated into completion criteria. Ultimately, these ensure that your security project plan provides the requisite level of security and complies, where necessary, with laws and regulations such as Sarbanes-Oxley and others.

After completing your WBS, you should perform your first scope check. It's here that you discover whether your scope and the tasks defined in your WBS are aligned. In most cases, there is some sort of mismatch and, therefore, you have an opportunity to work through these disconnects fairly early in the planning stages.

We discussed the importance of developing task details and how these details can be used to enhance security and ensure your project delivers the quality results you require. It's important to have subject matter experts participate in developing the WBS and the task details, since they are closest to the technical details and are the ones best suited to developing meaningful task details and metrics.

Project constraints in an IT security project plan are slightly different because legal, regulatory, or industry requirements are constraints not always found in other kinds of IT projects. Be sure to include all legal, regulatory or industry requirements not only in your task details, but also in your constraints. These are likely to shape the way your project proceeds, and should be addressed at the outset of the project planning phase.

Testing is an important element in IT security and it's vital that your project plan include test procedures. In some cases, this can be accomplished via task details and completion criteria. In many cases, however, it also requires you to test down through the ISAP and across the enterprise

to ensure there are no gaps in security. Some organizations and projects require a separate IT security test project plan, others simply require that discrete testing tasks be built into the project WBS.

We looked at the areas where the ISAPs and the corporate IT security project plan come together. In later chapters of this book, we'll look at some individual security area project plans and step through them. However, it's important to understand that there may be two discrete types of plans you're working with; the corporate IT security project plan, which addresses the entirety of corporate IT security, and the individual security areas like wireless security or operational security. These areas are sometimes implemented as individual projects, but must also be viewed as part of the larger whole. We looked at aspects related to both the corporate IT security project plan and the individual security project plans as it pertains to the critical path, budget, schedule, and risks. We finished the chapter with the four C's discussion, reiterating the importance of communicating clearly, concisely, and consistently.

Solutions Fast Track

Creating the IT Security Project Work Breakdown Structure

- ☑ The WBS is developed from the three to five major objectives identified in the definition phase of the project.
- ☑ Use a numbering system to help manage tasks. You can later refer to them by number rather than name to lend clarity to your communications.
- ☑ Your WBS may include the tasks from your sub-projects, or it may include just the corporate IT security project plan tasks.

Defining Project Tasks and Sub-tasks

- ☑ Tasks should follow the 8/80 rule. If they are shorter than 8 hours, roll them up into another task (if possible). If they are longer than 80 hours, split them into smaller tasks.
- ☑ Tasks and sub-tasks are often identified in a linear manner, but should not be placed in a formal order. The final order for tasks will be based on the logical flow of the tasks as well as the dependencies and constraints.

Checking Project Scope

- ☑ Once you've identified all of the project's tasks, you can check the scope of the project.
- ☑ It's common to find that the WBS defines work that is larger than the defined (or desired) scope of the project. Either you'll need to reduce your WBS task list, or you'll need to adjust your scope statements.
- ☑ This is typically the genesis of scope creep, so this is your first and best place to address potential scope creep.
- ☑ Often the process of creating the WBS causes you to discover additional information germane to the project planning process. This often causes you to have to reevaluate your scope.
- ☑ If your scope has legitimately changed based on the information you've discovered, discuss the proposed changes with your project sponsor.

Developing Task Details

- ☑ The task details can include all kinds of data. For an IT security project, it should include functional and technical requirements, as well as any legal, regulatory, or industry requirements.

- ☑ Your completion criteria should include legal, regulatory, or industry requirements. When each task is completed according to specifications, there is a much higher likelihood that the project results will also be compliant.
- ☑ Gather lessons learned as part of the task detail. This may help team members avoid common pitfalls or leverage new streamlined methods.
- ☑ Regularly reviewing lessons learned helps share knowledge earlier in the project lifecycle. Waiting until the end of the project to gather lessons learned, misses an opportunity to improve the project and risks missing the opportunity to capture organizational knowledge.

Identifying and Working With the Critical Path

- ☑ By definition, the critical path is the longest, least flexible path through the project.
- ☑ When dealing with tasks from both the ISAPs and the corporate IT security project plan, you may have more than one critical path to deal with.

Testing IT Security Project Results

- ☑ Testing plans should be developed in the planning phase of the project.
- ☑ Tests should include testing the security or the result of individual security tasks.
- ☑ Tests should include testing the security in an individual security area plan (ISAP) as well as across the enterprise.
- ☑ Test plans may be implemented as separate projects or as part of the project's existing WBS.
- ☑ Test plans can include unit testing; integration testing; usability testing; acceptance testing; beta testing; regression testing;

performance testing; stress and load testing; stability and reliability testing; and benchmark testing.

Budget, Schedule, Risks, and Communications

- ☑ The budget for ISAPs and the corporate IT security project plan must be addressed individually and as a whole. Gaps or omissions in your budget can be difficult to resolve later.
- ☑ The schedule for ISAPs and the corporate IT security project plan can be challenging to manage since you have several potentially conflicting demands for resources.
- ☑ Some tasks can be run in parallel, but be sure to look for resource constraints and conflicts if you do so.
- ☑ Risks to your project involve the risks to the ISAPs and the combined risks of the projects. Some risks span ISAPs and should be addressed and managed as such.
- ☑ Remember the four C's: communicate clearly, concisely, and consistently. Successful projects are as dependent on the perception of success as on the actual outcomes.