Chapter 2

Defining the Security Project

Solutions in this chapter:

- **Defining the Security Problem**
- **Defining the Security Mission or Outcome**
- **Defining Potential Security Project Solutions**
- **Defining the Optimal Security Project Solution**
- **Applying Security Project Constraints**
- **Developing the Security Project Proposal**
- **Identifying the Security Project Sponsor**

☑ **Summary**

☑ **Solutions Fast Track**

Introduction

This chapter discusses the initial steps for creating an Information Technology (IT) security project plan using standard project management methods. This chapter introduces the concepts you need to create both the overall corporate IT security project plan and the individual plans (ISAPs) that you'll find toward the end of this book beginning in Chapter 9. As we step through the project management elements in this chapter, we're going to keep it short and sweet because each of these elements will be repeated again in each of the security project plans included starting in Chapter 9.

Defining the Security Problem

The first step in developing a solid IT security project plan is to define the problem. We can easily state that the problem is that "our networks are not secure or that there are assets in the organization that need to be protected from intentional and unintentional attack." Those statements are true on the macro level, meaning that these general statements apply to almost every organization (and computer) in the world. However, every company is different and every organization has its own unique set of security vulnerabilities to consider. Applying a one-size-fits-all approach to network security will simply not work.

As discussed in Chapter 1, an effective way to approach IT security is to create a corporate security plan that includes the individual focus areas of security (e.g., infrastructure, wireless). Breaking down each of the segments into smaller, individual focus areas allows you to better manage each aspect of security. Another challenge you will encounter is that there are many areas that overlap (i.e., does physical access fall under operational security, infrastructure security, or general security?) Creating a corporate IT security plan and individual plans gives you the opportunity to review your overall security project plan to ensure that all critical security elements are addressed.

Let's begin with a review of some of the industry's standard definitions and focus areas of security that you can use to create your security project plan.

Network Security and the CIA

An easy way to begin looking at network security is via the well-known acronym "*CIA*" which stands for *confidentiality*, *integrity* and *availability*. These are the three overarching areas of network security that touch upon every network component from firewalls to user passwords. Let's look at these in detail so you can begin formulating your network security problem statement.

Confidentiality

Confidentiality refers to preventing the unauthorized access, disclosure, and use of information, and is part of the broader concept of privacy. Every company has different confidentiality needs (e.g., a hotel must keep guest room and credit card numbers and home addresses private; a beverage company must keep its product formula secret; an online retailer must keep customers' shopping data private; and an online search company must keep the user search data private).

Confidentiality is maintained through user authentication and access control. User authentication ensures that the person trying to access the data is authorized. Access control is the process of defining which users and groups should have access to the data. In combination, these mechanisms help ensure the confidentiality of data; however, there is little you can do to guarantee confidentiality without the users' participation, agreement, and compliance. User awareness, training, and education are vital components of any security solution, and typically part of a company-wide awareness, training, and education initiative. In the larger scheme of things, confidentiality has to do with how users handle and

utilize confidential data and these are often elements of regulatory issues such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA). These are typically part of a company-wide awareness, training and education initiative in which the IT department should participate.

Integrity

In the IT world, *integrity* refers to the reliability and trustworthiness of the information. *Data integrity* refers to the need to retain or preserve the information (without alteration or corruption) from source to destination. *Source integrity* refers to the verification process that is involved in ensuring that the data came from the correct source rather than from an imposter or a "man-in-the-middle (MITM)." Finally, integrity also refers to whether or not the correct data was initially entered, and whether the calculation or action will yield the same result each time.

While there is a "user" component to integrity, securing the network so that data and the sources of data cannot be altered is an IT function.

Availability

Most companies rely heavily on computers and networks, and the data that resides there. *Availability* is a critical function for companies that rely on electronic data and communications. Like data and network integrity, availability is an IT function (e.g., making sure the network is up and running, the data is available to the right users at the right time, the Web sites and Internet resources are available to the appropriate parties). Your IT security plan must also account for when users inadvertently lock up records in a database, server hard drives crash, routers fail, or hackers hack.

CIA in Context

How much security is enough to ensure CIA? To answer this question, we use this analogy: "How much security do you need in your personal life?" A lot of people that live in the country know their neighbors and do not lock their cars or homes. Contrast that with people who live in

urban settings where cars are stolen and homes are burglarized. The amount of security the city dweller needs is different than what the country resident needs. The point is, you cannot decide how much security is enough without first putting everything in context. The same holds true for companies. We all expect our bank to have extremely tight security not only because of the risk of financial loss but the potential for identity theft as well. A manufacturer of screen doors may have a fairly low need for security because they may not handle data much more complex and confidential than last year's sales numbers. Granted, you may not want these publicly divulged (if you're a privately held firm), but you wouldn't implement the same types of security systems your bank should. In Chapter 3, we'll discuss developing project objectives and we'll specifically talk about the security assessment. A security assessment (or audit) will help clarify the specific problem areas in your organization so that you can fine-tune your security project plan to address any shortfalls.

Business Intelligence…

One Size Fits None

It is very important that you to take the time to clearly define your organization's unique security profile before implementing any plans or solutions. There are thousands of companies selling all kinds of security solutions. Clearly, some are better than others, but more importantly, some are more appropriate for your company than others. You need to determine how much time, money, and effort should be expended to develop the appropriate security solution. If you do not have a clear idea of your security needs before you start shopping for hardware, software, or a security consultant, you may be talked into a solution that is too big, too small (rarely), too expensive, or not appropriate for your firm.

Define the Problem

Now that you have an overview of the major security elements to be considered, you can begin to define your IT security project plan problem statement. The information you considered as you read the previous section should have helped you begin to see how you can define your problem statement. While yours will be unique, we've provided a few samples for you to use as starting points. Be sure the problem statement matches your organization's real needs. Be sure you're focusing on the overarching corporate IT security plan. We'll work on problem statements in the smaller, more focused security plans later in the book. The sample statements below are just starting points. You don't need to spend days thinking up your problem statement, but you should hit the major points. As we continue to refine our project plan, we'll continue to add detail to the plan that should help you address all needed areas of IT security for your firm. Don't add the "laundry list" here, try to create a clear, concise overview of the corporate IT security situation that is causing you to take on this project. While your security project plan will be unique to your organization, the following are good starting points:

- My company works with highly confidential data that is currently exposed to potentially inappropriate internal and external access, use, and distribution.
- My company lacks a comprehensive approach to IT security, and the network assets are at risk. There is no system in place to ensure that only authorized users can access confidential data. We also lack a consistent method for monitoring network access to certain resources.
- My company's security measures were put in place on an "as needed" basis; we have never done a comprehensive review of the security measures. Since the company has both internal and external employees that access confidential data while working remotely, we need to ensure that our security policies and practices protect the corporate assets.

As you can see, it doesn't take a rocket scientist to write a problem statement that will get you going. If you're a detail-oriented person, you might want to define your problem more specifically. However, at this point, we're really just taking a high-level look at the problem. Later, we'll dig into the detail because part of every IT security project plan is making an assessment of the current network and current security measures. Rather than repeat that, we'll mention it here and return to it later.

Defining the Outcome

If you know what the problem is, you can identify the desired outcome. This is where you begin defining how much security is appropriate for your organization. If your security meets the highest level of government security standards, you are setting the bar extremely high. However, if your company is a regional retailer of shoes, it is probably too much security. Taking the time to clearly identify your desired outcome can help you define the right level of security for your organization. Your security project plan should incorporate elements specific to your network and to your company. The mission statement defines what the overall end result should look like. The following are good starting points.

- Our security solution should take into account the need to secure all network data. We must be compliant with the Health Insurance Portability and Accountability Act (HIPAA) standards. Our security solution should prevent unauthorized access at all branch locations, and monitor access to confidential data files. Our auditing systems should be able to spot unusual access or traffic patterns.
- Our security project plan should secure corporate network resources while providing customers with fast and easy access to the Internet through our wireless network connections.
- Our firm requires extremely high data security to prevent unauthorized access, use, retrieval, sharing, forwarding, removal, or modifica-

tion of confidential research and development data. If this data were stolen by competitors, the financial losses would be staggering and could potentially put the company out of business.

- The desired outcome is to provide a reasonable level of security for the network while keeping administration and day-to-day monitoring tasks to a minimum. In addition, we want to prevent unauthorized network access, virus infection, and malicious software (malware) installation.

As you can see, these statements vary greatly. The last one indicates that a less rigorous security solution would probably be just fine. The first item indicates there are potential legal ramifications (HIPAA) of a security breach. This would indicate a need for a stronger security solution. Matching the value (tangible and intangible) of your company's data and the severity of the impact of a potential breach or outage with the proposed solution will help you define the optimal solution for your company.

Defining Potential Security Project Solutions

In traditional project management, once you have defined the problem and the desired outcome, you begin thinking about potential security project solutions, which is done by brainstorming ideas and narrowing the resulting list down to the solutions that fit both the problem and the outcome. The list of choices is further narrowed by looking at which potential solution is the most viable for your specific circumstances. In this case, you cannot identify potential solutions until you identify the required components of security. The objective at this stage is to identify (at the corporate IT security project level) the relative scope of your project. Another potential solution might be to hire a security expert, or you might decide to send one or more IT staff to

security training programs. The reason you're spending time looking at this is to help you develop an idea of the scope of your project and the possible solutions you could employ. If you don't spend time reviewing all potential options, you might miss finding the most optimal solution possible. Don't start from a limited point of view, start from the position that "all things are possible" and we'll narrow down the choices later.

Keep in mind that your security solutions will be modular. What is appropriate for your overall corporate IT security solution may not be appropriate for individual security project plans. A good solution may be to hire a security consultant to do an extensive security audit and make recommendations. However, your optimal solution for the wireless security plan will be different. If you have no expertise, you should hire a consultant to implement your wireless security plan and train your IT staff. If you have a lot of experience, you might hire an outside consultant just to review your staff's plan.

The key here is understanding that different segments of the plan, while interrelated, should be addressed individually. The optimal solution for one security area might not be right for another. Your optimal solutions should be based on your company's business, industry, current infrastructure, and risk profile, as well as your IT team's proven expertise. Take an unbiased look at the optimal solutions so that you can develop the best solution for your company.

Defining the Optimal Security Project Solution

At this point, you understand your overall security problem and the desired outcome. You've looked at all possible security solutions and made a list. Now, you need to review your list of possible solutions and narrow it down to the most optimal solution. Notice we still haven't identified or considered constraints such as time or money. If we start with limited options, we might miss finding the best option, so we start

with all possible solutions and look for the very best one given what we know about our company. For example, your company may have a culture that supports hiring the best and the brightest, then your best solution might be to go find the best IT security person on the planet. If your company is always running on a shoestring or has a culture that supports "homegrown" initiatives, you may choose to hire or train IT security staff.

You may not be able to identify the optional security solution until you do an assessment. IT project management is an iterative process; as you receive new information, you have to make modifications to previous definitions.

The good news here is that once you've done all this high level work for your corporate IT security project, it will be easier to do these same steps for your smaller, individual security area project plans.

Applying Security Project Constraints

You have looked at optimal options, and now you have to adjust your plans accordingly. Every project has four constraints: scope, time, cost, and quality. If your IT security budget is slashed by 25 percent, you will have to adjust your budget accordingly. If you reduce cost, you will typically have to reduce the scope, quality, or increase time. Quality is often sacrificed, which can have serious consequences in the security arena. You will have to make some hard decisions. The following sections review the security project plan constraints and how they apply to your corporate IT security master plan and your individual security project plans.

Scope (Amount of Work)

The *scope* is the total amount of work to be accomplished. If you have a tight budget, you may decide to focus on the three major security areas that will be the foundation of your security project plan (i.e., identification and authentication, auditing, and malicious code protection). You

may also decide to define several phases so that you can cover the most pressing security needs first, and then add additional elements in smaller security project plans. Choose your scope carefully to ensure that the corporate assets are covered. If your scope does not cover the most important and vulnerable assets, you may have to request a larger budget (see Chapter 1). One of the worst mistakes you can make is defining, planning, and implementing a security plan that does not cover the key areas. If you cannot implement the security project plan necessary for your company, document the risks and bring it to your manager's attention. Make sure the decision makers know what the impact of their decision will be on the IT department. They rely on your expertise; if you silently accept budget or timeline cuts, you are doing your company a disservice. Be professional but clear about the implications of failing to implement the full scope of a security project plan.

Time (Schedule)

Everyone always wants projects completed as quickly as possible. Every project requires a certain amount of *time* to complete. A schedule is developed after you define the work to be accomplished and compile the necessary resources. If you have to shorten your schedule, you might have to reduce the project's scope and quality, or increase the budget to allow you to purchase additional time-saving tools or hire additional staff. In traditional project management, there is the concept of "crashing the schedule," which means running things in parallel. In security project plans, the danger is in leaving a gap or making an error. As you go through the project planning process in this book, assume that "crashing the schedule" is not an option. In addition, make sure you allow plenty of time for testing, which is one of the best quality control tools you can use. You may also choose to hire additional staff to test your security solutions and to purposely look for ways to break your security.

Cost

IT departments are being asked to do more with less money, even as IT budgets have increased. The amount of spending on security is, on average, approximately 5 to 10 percent of IT budgets, which is not much when you consider the cost of a security breach. If you are forced to reduce your budget, you will have to find creative ways to address the shortfall (e.g., "borrow" staff from other departments, re-use or re-purpose tools you already own). If your budget is cut, you will have to reduce the scope or the quality of your project. Also, the amount of time the project takes might have to be reduced to address the budget issues, or you might have to increase the amount of time needed to complete the project in order to avoid overtime costs.

At the risk of repetition, be very careful about agreeing to implement a security plan that lacks sufficient scope, time or money. At the end of the day, everyone will forget what the agreed upon scope, budget or schedule was and they'll come looking for you when that security breach occurs. No one will remember the discussion you had six months ago about the risk of implementing a lower cost security plan. What they'll remember is that you and your team implemented the plan and it didn't work. Of course on the flip side, if you successfully implement a plan and no security problems ever occur, don't expect a pat on the back or a letter of congratulations. The absence of a problem is rarely rewarded, but at least you and your team will sleep better at night knowing your network and corporate data are as secure as they reasonably can be.

Quality

The quality of an IT security project plan often comes down to the amount of testing and review that is done prior to, during, and after project implementation.

Now that you have reviewed the project constraints for your IT security project plan, you can compare them to your optimal solution and revise it as needed. If your optimal solution is too expensive or will take too long, you will have to modify your solution to fit within the project constraints. Conversely, if you feel strongly that your optimal solution is exactly what your company needs, prepare a brief document outlining why this security solution is the right one for your company and why the resources should be expended to implement it. Be clear, concise, and factual. Document the risks associated with *not* implementing the optimal solution, so that your manager or the company's executive team can make an informed decision. Clearly delineate the risks of not implementing the best solution for your company.

Finally, it is important to note that you may not know exactly what your security project plan constraints are at this juncture in the security project planning process. Some companies require a proposal, the assumption being that the more impressive the proposal the bigger the budget. In some cases, you cannot write an intelligent proposal until you understand the constraints. If you do not have specific data regarding your IT security project's constraints, list your assumptions. That way when you submit your proposal, you have a starting point with which to negotiate.

Business Intelligence…

Setting Security Priorities Based on Constraints

In a perfect world, we would have all the time, money, and resources needed for our projects. The reality is that there are always limitations to contend with. As you begin defining your security project plan and understanding the project constraints, you will get a better idea of the project's constraint priorities (e.g., if you are told you need to implement a security plan quickly, you might believe that the highest priority is time (schedule). If that is the case, you either have to reduce the scope to finish the security project plan quickly, or you have to increase the

Continued

budget to hire additional staff to help plan and implement the project. However, don't assume that because you keep hearing how quickly this project needs to happen that time is the highest priority. In fact, cost might still be your highest priority in terms of what to focus on even though everyone's harping on time.

To verify your assumptions you can test the waters by asking, "If we need to get this done quickly, I'm assuming we'll have a budget that supports overtime and hiring outside help. Is that correct?" If you believe budget is the priority, test the waters by stating, "Since we are working with a limited budget, the amount of work we can get done will also be limited. I'm assuming that is acceptable." These kinds of tests help you push the boundaries to find out where the real limitations are. You need to understand the priorities so that when push comes to shove, you will know on what basis to make decisions. To run a successful project, you need to know how to allocate resources and how to make decisions based on priorities. If cost is the primary constraint, you might increase the length of the security project plan or decrease the scope. If time is the primary constraint and you incorrectly assume that cost is the constraint, your decisions will create problems for all concerned.

Developing the Security Project Proposal

Once the preliminary work is done, you can develop a security project proposal and use it to negotiate a bigger budget or a longer timeline, or to discuss security project constraints. In either case, develop a security project proposal that will be the basis of your overall security project planning. This document should contain the following elements, at minimum:

- Project name
- Proposal date
- Project manager
- Problem statement

- Mission or outcome statement
- Proposed solution
- Project constraints (if known)
- Desired security project completion date
- Initial proposed Budget (if known)
- Other relevant information

Once this proposal is developed, bring it to your security project plan sponsor for approval. The format of the proposal depends largely on what is generally accepted in your firm. Some companies have a formal culture that requires a printed, bound document be provided to the security project plan sponsor. Other companies have an informal culture where a quick e-mail might suffice. Regardless of how the proposal is captured, be sure that two things occur:

- The proposal is written clearly and concisely.
- The proposal is discussed in real time (face-to-face is best; phone is acceptable).

If you don't write the proposal down, you have no record of your starting point. If you simply submit the proposal without also talking with your project sponsor about it, you risk having misunderstanding right from the start. Let's talk about the role of the security project sponsor in this type of project.

Identifying the Security Project Sponsor

A security project sponsor is the person who champions the security project plan within the organization. He or she is typically high enough in the organization to have the authority to help remove or reduce the roadblocks that your security project plan will invariably run into. The security

project sponsor can be your direct supervisor or the president of your company. The role of the security project sponsor is to approve the security project plans, budget, and schedule, and help provide resources for the project. If he or she is not motivated to help ensure the project's success, your project will probably run into problems down the line. If you suspect this is the case, find someone else to be your security project sponsor who will partner with you for success (and who has the political pull in your company to get things done).

Once you have identified a security project sponsor, start off by sitting down with him or her and discussing your initial security project proposal, including your assumptions regarding security project constraints. This is also a great opportunity to develop a better relationship and a clear and mutual understanding of the proposed project. If everything is in sync, you are ready to write your security project proposal. If things are not in sync, determine if you need to clarify it, incorporate feedback from your security project sponsor, or go back to the drawing board. Whatever the outcome, if your security project sponsor does not make time to talk with you at this early stage, it should be a warning flag and you should re-think your approach (e.g., find a new sponsor, find a new method for scheduling meetings with your sponsor).

This is also a good time to clarify how you and your security project sponsor will interact and work together. Some people prefer quick e-mail updates, while others prefer a regularly scheduled, face-to-face meeting. Your job as IT security project manager is to ensure the project's ultimate success, which means that you may have to bend a little to achieve your objectives. If your security project sponsor wants an in-depth, detailed, blow-by-blow update on a weekly basis, you will either have to provide it or suggest a suitable alternative. Take time at this juncture to determine how you can best collaborate with your security project sponsor to achieve your ultimate goal—a successful project.

Summary

All security project plans should begin with a clear definition of the problem, the outcome, the possible solutions, and the optimal solution, which will set the foundation for success. Remember, smaller projects with smaller scopes, shorter timelines, and more milestones are typically more successful. This method works well because it helps you focus on the overall needs of the company first, and then provides a method for looking closely at the individual security areas.

Solutions Fast Track

Defining the Security Problem

- ☑ All projects should start by defining the problem to be solved. If you cannot state the problem to be solved, you need to give additional thought to the subject before proceeding.
- ☑ Confidentiality, integrity, and availability (CIA) are the three areas that security must address.
- ☑ Additional security data regarding known security problems are addressed in the security assessment performed later in the process.

Defining the Security Mission or Outcome

- ☑ The mission or outcome statement should state the desired or required result of your security project plan.
- ☑ At this stage in the planning process, the statement should describe the outcome desired (or required) for your corporate IT security project plan. Individual security topic areas will be defined later.

- ☑ If you cannot state the desired outcome clearly and concisely, you may not have a clear idea of what you are trying to achieve. Clarity at this stage of the planning process is critical to success.
- ☑ Defining the problem and mission should take a relatively short time.

Defining Potential Security Project Solutions

- ☑ Your planning process should include a brainstorming session to identify all possible security solutions.
- ☑ Do not filter solutions because they initially seem to be too expensive or too innovative. List all solutions at the outset.

Defining the Optimal Security Project Solution

- ☑ Look at all potential solutions and decide which one appears to be the optimal solution. It is not always the first solution you think of.
- ☑ Be sure the optimal solution fits the problem and mission statements.

Applying Security Project Constraints

- ☑ Every security project has four constraints: scope, time, cost, and quality.
- ☑ Review your optimal solution in light of the known security project constraints.

- ☑ Since constraints are not always known at this juncture, list any assumptions you have made about security project constraints so that you can verify them later.
- ☑ Be prepared to discuss the security project constraints based on your security project proposal. If you state the business case clearly, your higher budget or longer schedule may be approved with little push back.

Developing the Security Project Proposal

- ☑ Be sure to capture the key elements of the security project proposal. This includes security project name, project manager, date, problem, mission, potential solutions, optimal solution, and constraints (known or assumed).
- ☑ The proposal can be formal or informal, depending on your company's culture.
- ☑ Be sure to have the proposal approved by your sponsor before proceeding.

Identifying the Security Project Sponsor

- ☑ The security project sponsor can be your supervisor, manager, or a company executive.
- ☑ The security project sponsor approves the security project plan, budget, and schedule, and helps clear roadblocks to the project's success.

- ☑ The security project proposal is the first opportunity you have to check and align expectations with the security project sponsor.
- ☑ Schedule a meeting with the security project sponsor to discuss the initial proposal.
- ☑ If your security project sponsor is too busy or unwilling to participate, try to find a new security project sponsor. A good security project sponsor can pave the way to success; a poor security project sponsor can create roadblocks and delays.
- ☑ Take time at this juncture to understand the best way to communicate with your security project sponsor. Setting clear expectations now will save time later.