Chapter 3

Organizing the IT Security Project

Solutions in this chapter:

- **Identifying the IT Security Project Team**
- **Identifying IT Security Project Stakeholders**
- **Defining IT Security Project Requirements**
- **Defining IT Security Project Objectives**
- **Defining IT Security Project Processes**

☑ **Summary**

☑ **Solutions Fast Track**

Introduction

All projects require organization before they can be fully planned and implemented. This chapter looks at some of the most common methods used for organizing Information Technology (IT) security project plans. Once the organizing phase for the corporate IT security plan is complete, we will begin identifying the details of the project.

Project planning and management are iterative processes. This chapter steps through the numerous processes that are part of organizing an IT security project plan. However, that being said, you may not be able to clearly articulate some of these elements until you have done additional work (e.g., you cannot clearly define all of your IT security project requirements until you have performed a network risk assessment or thorough audit). Sometimes in the planning phase, you cannot define certain elements until you have gone a few steps further in the process. If there are elements you cannot define, create a placeholder and go back to them when you have more detail. Also, you may need to complete one or more individual security area project plans before you can finalize your overall corporate IT security plan.

Identifying the IT Security Project Team

There are often two distinct groups within a project team: one helps with the definition phase and the other one implements the project. Typically, the definition phase of an IT project requires outside input, which is where many IT projects start to go bad. A lot of these phases are planned in the back of the server room by IT staff, which is fine if you are discussing something purely technical; however, IT projects impact many others beyond the IT staff.

A successful project, as you'll recall, involves users and appropriate stakeholders (see next section) early. One of the best ways to make sure you avoid re-doing a lot of planning work is to include users on the initial project team. Just because they are part of the initial team doesn't mean they have to be on the implementation team, though it's often a good idea to include a few users/stakeholders on that team as well. During the planning phases, key users should be selected for their ability to add value to the process, not for political purposes (though we all know you sometimes have to accept the 'political appointee' graciously). Getting users involved can create critical mass for your project and if well-managed, it might even generate user commitment because you'll have key staff championing the IT project to others in the organization. Participating in creating something usually creates that all-important "buy in" and you'll need your users to be on board with any security project so this is as good a place as any to start. Keep in mind that IT staff often misunderstand the needs of the users and users almost always misunderstand the IT function, so be prepared to do a bit of educating (and a lot of listening) along the way. The more opportunities you have to educate users on how things in the IT world work, the more effective you can be in meeting user's needs. The more opportunities you can take to really understand what users need, the more effective your IT projects will be.

Some projects benefit from users being involved in the process. You may decide to have subject matter experts from key user areas participate in the entire project. In a security project, there will be pieces a user does not understand (e.g., encryption). On the other hand, a user can provide a great reality check when you are deciding between smart cards or a 10-step logon procedure.

Create clear criteria for selecting the right people for the project. Avoid inviting people that are not critical to a successful project. Also, keep the project team as lean and mean as possible to make it easier to manage.

Identifying IT Security Project Stakeholders

Stakeholders are the people who are impacted by a project or who impact projects. It is always a good idea to find out who may be impacted before going too far into the planning stage. If you overlook this step, you will invariably receive additional information later in the planning cycle that will cost more time, money, and effort. Consider this: Suppose you are well into your security project (you may have even begun implementing it), and you find out from Human Resources that there is a new government regulation that your company must comply with. You also find out that Human Resources knew about it three months ago but did not know that it would have an impact on the IT group. Now you have to go back and redesign part of your authentication project plan, because it does not take the new regulation into account.

At the outset of the IT security project planning process, have a meeting with key members of every department that is present. Create a brief presentation using your project proposal (see Chapter 2). Explain what you are trying to accomplish and find out who should be involved in the project planning. There are often key people outside of a project implementation team that should be included in both the planning and testing phases. Once everyone knows about your project, follow up with an e-mail to those same parties asking them to respond to some short questions. The questions should be designed to ask if there are any department-level considerations that should be included in the planning process (e.g., finance might indicate they do not need to participate; however, you want someone to help you understand what types of data the finance department works with, how sensitive it is, where it is stored, and so on).

One way to categorize stakeholders for an IT security project is to determine who must be *involved*, who might be *influential*, and who must be *informed*. Those who should be involved are those who will either provide critical input to the project, or be directly affected by the results of the project. Influential stakeholders should not be overlooked because they can be key to gaining support for the project and keeping corporate resources focused on achieving the project's objectives. Influential stakeholders are often project champions within an organization; therefore, utilize them whenever possible. Finally, there is a group of stakeholders that should remain informed, which includes the executive team, and may also include key stakeholders who were part of the initial planning and who may need periodic updates to fulfill corporate or government reporting requirements. This is especially true if your IT security project plan touches on industry or governmental requirements such as SOX or the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

The following is an initial list of potential project stakeholders who should be represented on your IT security planning team:

- IT staff
- User representatives
- Human Resources
- Finance
- Legal
- Departmental managers
- Regional or site managers

Defining IT Security Project Requirements

Security project plan requirements are not defined until the stakeholders are identified; however, a preliminary set of project plan requirements can be created. The key is making sure you get the stakeholders' input before finalizing your security project plan. If you fail to involve the stakeholders, you will end up with a security project plan that is missing key requirements, or is difficult or impossible to implement or maintain.

Project requirements are those elements that your security project plan must incorporate. There are four categories of requirements: *user*, *business*, *functional*, and *technical*. Requirements can also be analyzed in the following way:

- **User Requirements** What do end users need to help maintain a secure network environment?

- **Departmental Requirements** What do the various departments need for security? Human Resources needs tight security on personnel files; Accounting needs tight security on credit card numbers and company financials; and Business Development may have specialized security needs related to staff that travels frequently.
- **External User Requirements** Are there vendors that need to connect to the network? If so, what are their needs? Do you provide customers the ability to get real-time data online, and if so, what are their requirements? Does your company allow employees to connect to the corporate network from home or on the road? How should these external connections be protected?
- **Corporate Policy Requirements** Are there any corporate policies that can be interpreted as requirements for an IT security project plan? If so, put them in your security project plan.
- **Governmental Regulation Requirements** Is your organization subject to Sarbanes-Oxley (SOX) regulations, Health Insurance Portability and Accountability Act (HIPAA), or any other governmental regulations that could impact your IT security project plan?

You may have other requirements relevant to your industry, business activities, location and more. This is not an exhaustive list but just a starter to get you thinking about all the requirements. As you can see, this is where having representatives from different parts of the organization can really help you out since there may be numerous requirements that should be addressed.

In addition, consider the project constraints (scope, time, cost, and quality) as project requirements (e.g., some IT project managers include the initial project constraints if there are specific requirements). If your budget for the security project plan is $25,000, you might include it as a requirement. In the early stages, it is better to include elements that you may later determine you do not need, than to inadvertently overlook an important requirement.

Requirements are the elements that a security project plan must provide. If you do not involve your stakeholders in defining the IT security project plan requirements, you may end up with a project that fails to meet stakeholder requirements, which can result in project failure. When you put up firewall security so secure it is impenetrable, you think your project is a success, until you begin receiving user complaints such as they cannot utilize the Internet or share files with customers or vendors. The perception of the success of the project has just plummeted. You have met IT's security requirements, but failed to take user requirements into consideration.

To effectively gather stakeholder requirements, hold an initial project meeting. Invite all potential stakeholders and work with them to identify as many potential requirements as possible. Once you have compiled an extensive list, pare it down and circulate it for approval. When you state the requirements that the security project plan must achieve, you have identified the scope of the project. If your list of requirements is too long or varied, consider breaking it down into several smaller security project plans. You will probably have to reduce the requirements to a manageable subset before proceeding to the formal planning stages. Reducing requirements is a way of managing the scope; if you do not define and manage your requirements throughout the project, you will have a bad case of *scope creep,* a term used often to describe uncontrolled changes in a project's scope. To help avoid (or minimize) scope creep, create a clear set of the requirements necessary to create a secure environment.

The reverse situation can be equally challenging. Suppose you invite a number of key stakeholders to a meeting to gather IT security project plan requirements, and no one comes? Or, suppose a number of people come that have no meaningful input? At that point, you would need to explain the necessary requirements before continuing the meeting.For example, you might distribute a list of possible requirements via email and ask them to respond. You may have to get creative but don't simply accept that the users have no requirements if they fail to deliver them. They have requirements and it's up to you to ferret them out prior to finalizing your project plan.

Business Intelligence…

Taking the Pain Out of Meetings

People hate boring meetings, and the truth of the matter is, many IT-related meetings are boring. Some IT staff are more comfortable interacting with computers than with users. Following are some tips to help facilitate communication at the meeting:

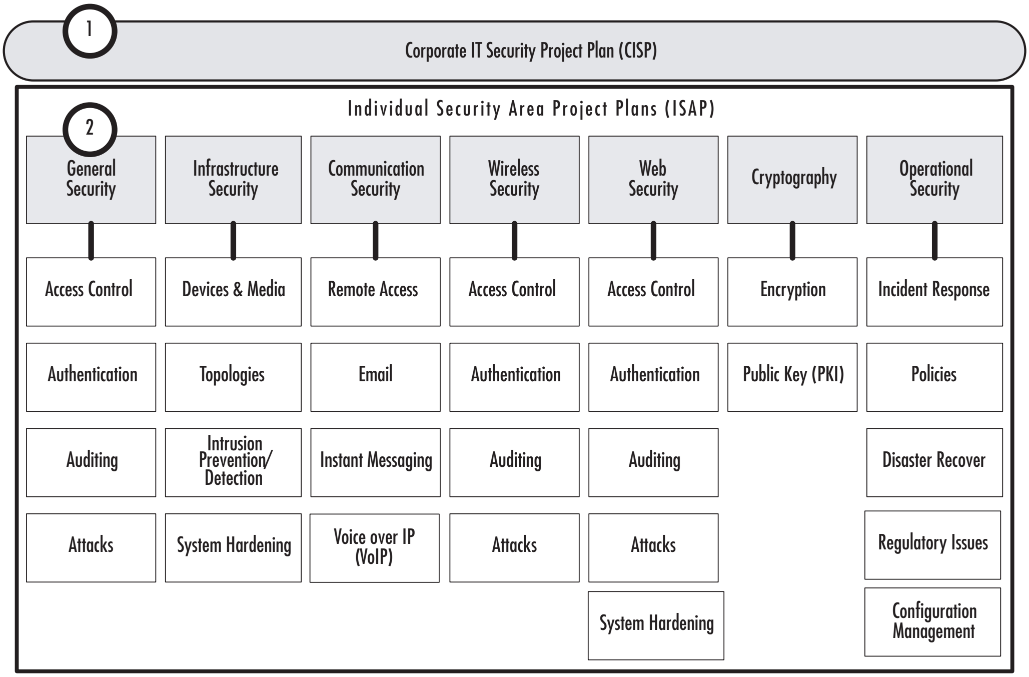
1. Decide what you want out of the meeting.
2. Plan the meeting from the user's perspective; try to anticipate how he or she will respond to the meeting and plan accordingly.
3. Have a Human Resources manager or a facilitator moderate the meeting. A facilitator can help keep the meeting on track, on time, and on topic. If your team does not have a facilitator, use company resources.
4. Be sure the users understand why they have been invited to the meeting.
5. Avoid "planning by PowerPoint." PowerPoint presentations should not be considered security project plans. However, PowerPoint presentations are an effective communication tool that can be used to explain the project overview.
6. Publish a meeting agenda and stick to it. Having an agenda helps participants understand the preferred objective and can help keep the meeting on track. An agenda will also help ensure that the meeting's objective is achieved.
7. Assign owners for follow-up items. If your meeting requires follow up, list the tasks, the due dates and the owners, and then follow up with them.

Defining IT Security Project Objectives

Once you have identified the stakeholders and compiled your requirements, you are ready to sit down with your team and begin developing the security project objectives.

After identifying the requirements, create three to five major objectives. The corporate IT security project plans and the individual security project plans each have different objectives. For ease of reference, they are referred to as the Corporate IT Security Project (CISP) and the Individual Security Area Project (ISAP). In Figure 3.1, the two levels of objectives are marked by the numbers 1 and 2. Number 1 indicates the CISP-level objectives and Number 2 indicates the ISAP-level objectives. You will create a distinct set of objectives for each of your ISAP plans; however, those objectives may overlap from one project to another.

Figure 3.1 IT Security Master and Sub-project Plan Objectives



The following is a sample list of CISP objectives:

- Provide a comprehensive security management framework for the organization.
- Provide a clear and consistent set of corporate security policies.
- Identify specific security areas to be reviewed and managed.
- Create specific ISAP plans to manage the appropriate security elements within the company.

ISAP-level objectives go into a deeper level of detail within the various security topic areas. Use the sub-items listed below each header in the ISAP section as the starting point of your objectives (e.g., under "General Security" in Figure 3.1, the following topics are listed: Access Control, Authentication, Auditing, and Attacks). These objectives can be stated as follows:

- Review, define, and implement access controls on the network.
- Review, define, and implement user and computer authentication.
- Define and implement auditing policies and procedures.
- Review vulnerabilities and develop prevention and countermeasures against attacks.

Everyone approaches things a bit differently, which is fine as long as everyone adheres to the underlying methodology. You want to define three to five major objectives that take into account your chosen project solution and requirements. If you find yourself defining 10 objectives, you are going into detail too early. Look at your list of objectives to see if one or more can be rolled up into a higher-level objective. On the other hand, if you only come up with two objectives, you may need to spend more time defining your project. Sometimes, if you only have one or two objectives, you need to break them down into more specific objectives. Three to five is a general guideline; some successful projects have three objectives, and some have eight. Make sure you double-check your objectives for your project plan. If your list of objectives is too long, you should consider breaking it into smaller sub-projects.

Defining IT Security Project Processes

Now we come to one of the large chunks of project definition that many people would rather skip. Let's face it – once the project is underway, processes will be used. They will be defined on the fly, they will be made up in the face of an emergency and they will almost certainly be less than optimal. As much as you probably don't want to do this (unless you're a real detail-oriented person), it really does help to define your project processes ahead of time. We're not going to delve too deeply into this topic but we will provide some helpful reminders to get you on track. Refer to your IT project management notes or references if you need a more in-depth refresher. The following is a list of project processes you should consider implementing for your project. If you aren't familiar with these concepts, you can review the IT Project Management material (see Chapter 1 for details on how to access this material). Your IT security plans should use fairly rigorous processes to ensure that your IT security project plan is airtight. We'll review each of these topics briefly with an eye toward IT security projects.

- Acceptance Criteria
- Risk Management Plan
- Change Management Plan
- Communication Plan
- Quality Management Plan
- Status Reporting
- Defect, Error, and Issue Tracking
- Escalation Procedures
- Documentation Procedures
- Approval Procedures
- Deployment Plan

- Operations Plan
- Training Plan

Acceptance Criteria

Acceptance criteria (sometimes called "success criteria)" are the criteria by which someone *accepts* results. Success criteria are the criteria by which someone deems the project a *success*. Though acceptance and success go hand-in-hand, it is possible that some projects may meet the acceptance criteria and still not be deemed successful. Numerous studies show that an IT project can come in on scope, on time, on budget, and with the required level of quality, and still not be deemed successful. Why? The most common reason is failure to communicate project status and progress. For our discussion, we use the term "acceptance criteria" to help keep focused on those tangible elements that can be measured and reported. Acceptance criteria such as, "users are able to log onto the network using the new required password format" is not a measurable statement. "100% of existing users are able to log onto the network using the new required password format on the first attempt," is both specific and measurable. Acceptance criteria typically address a project's requirements and are written in clear, concise, and specific ways to measure and quantify the project's delivery of the requirements.

Risk Management

There are numerous risks involved in developing an IT security project plan; therefore, it is important to spend as much time planning your project as necessary to avoid additional problems later in the process. Again, it helps to include key stakeholders so that you have an understanding of the risks of the project, which can run the gamut from, "What happens if we fail to implement?" to "What happens if we get bogged down in phase 2 of the project?" to "What are the financial and legal consequences of a failure in ISAP-level project 1, 2, or 3?" To help identify the potential risks, identify the following:

- What project risks must be managed?
- How much project risk is acceptable?
- How should those risks be managed (avoid, reduce, respond)?
- How will I know if those project risks are occurring?
- When should I implement my contingency plan?
- Who is responsible for implementing and managing the contingency plans?

You may need to create a security project plan for your network risk and threat assessment before developing a larger corporate IT strategy. You need to understand the unique threats to your network and corporate resources before you can create specific requirements for your security project plan. An audit can be a discrete project plan, or it can be incorporated into each IT security project plan.

Remember, too, that when we discuss risk management here, we're specifically discussing risks to the IT security project itself. Risk assessment from a network or data perspective is part of a threat assessment or security audit and is a separate process. In this phase, you need to understand what can go wrong with your project and how to deal with it. As with many other aspects of project management, risk assessment and planning ahead of project implementation can help save time, effort, and stress once the project is underway. By looking at what could go wrong before getting into the planning and implementation stages, you can find ways to avoid some risks and minimize others. Also, sometimes you will discover that your project plan is actually improved by the innovative ideas used to mitigate project risk.

Change Management

Errors and omissions in the IT security world create gaping holes that can be exploited, either unintentionally by users, or intentionally through internal or external attacks. Errors and omissions happen because changes to the security project plan are not managed well.

Managing change in an IT security project plan is a two-fold process. First, you have to identify the necessary changes and assess the impact these changes will have on your overall security project plan (e.g., will it impact your e-commerce application if you change how you configure your firewall). The second aspect of change management is keeping track of the changes. Changes should be incorporated and clearly documented into your security project plan (i.e., how, when, where, and why the change was made).

Successfully managing changes to a security project plan can mean the difference between success and failure. If you do not thoroughly assess and document those changes, you may not know which project plan elements were implemented, which will create security holes.

Business Intelligence…

Avoiding Endless Decision Loops

Some companies have a culture that encourages decisions be re-visited repeatedly. This is particularly true with project changes. For example: A team meets to discuss an unanticipated problem, brainstorm possible solutions, decide on a solution, analyze the potential risks of that solution, and determine how to incorporate that change into the security project plan. Two months later, someone encounters a problem that is related to the change, and the decision has to be re-hashed. No decision is reached and subsequent meetings are called to discuss the problem, which puts the project at risk. The project is endlessly delayed and rogue decisions are being made and implemented that are outside the formal security project planning process, which leads to "unspecified" results.

To avoid endless decision loops, document your change management process and use it faithfully. If you document everything you do, including the changes and the reasons for those changes, you can avoid the endless decision loops that delay projects indefinitely.

Communication

Communication is critical when you are planning your IT security project plan. Users can help secure the network by following the security policies and reporting suspicious activity.Your communication plan should address the communication needs of each stakeholder group.The communication plan is also an opportunity to distribute a positive message about the project and its progress.

Assess each stakeholder group individually and develop the appropriate communication plans (e.g., executives may want a high-level "dashboard" report on a quarterly or monthly basis, while users may want a more detailed understanding of how the project is going. If you are sending out long weekly e-mail updates, chances are good that most people will not read them. If you are printing out memos in a company that relies on e-mail, you are also missing your audience.The frequency of communication, the content of the communication, and the medium for communication are all important aspects of developing a successful communication plan for your IT security project plan.

Quality

In many cases, the quality of an IT security project plan can be measured, monitored, and controlled through testing.Your quality processes might include the level of testing required for each major security area in your security project plan. Moderate testing yields moderate quality, and extensive testing yields higher quality.The Federal Reserve Bank's banking system requires a higher level of security than a used book store; therefore, the cost to implement that security should be reflected. Lower quality is not necessarily a bad thing; however, it must be appropriate to the needs of your company.

Status Reporting

IT security projects have a unique set of demands for status reporting. As you begin implementing various security measures, you need to keep key stakeholders up to date (e.g., how much the project has cost to date, how the project is progressing against schedule). They may also want to know if particular parts of security have been modified or upgraded for governmental or corporate reporting purposes. Keeping key stakeholders in the loop is a bit of an art form. You need to ensure that you share important information regularly, supply the needed information in a clear and concise manner, and send updates on a regular schedule.

One successful method you can incorporate is to talk with the various stakeholders when you are defining project requirements, to help determine what type and frequency of update will be most useful to them. Information that is short, clear, concise, and well-organized is far more likely to be read and absorbed than long, rambling missives.

Defect, Error, and Issue Tracking

As with change management, defect, error, and issue tracking are important in IT security project plans. You can use whatever terminology makes the most sense to you in your organization (defect, error or issue), for clarity we'll simply call it issue tracking. Closely track issues related to your IT security project plan; not doing so may create huge security holes and gaps. Managing project issues is an important part of the project manager's job. Be sure you have a solid issue-tracking process defined in your IT security project plan.

Issues should be tracked to capture the source, the description, the owner of the issue, the agreed-upon resolution, and the timeline for resolution. Issues should also be assigned a unique identifier so that they can be found quickly.

Escalation Procedures

Escalation procedures are important for IT security project plans. If an issue cannot be resolved through normal channels, you need to have a pre-defined process for escalating it. This is where working with your sponsor and key stakeholders can be helpful, because they can lend you their organizational authority and help you create appropriate escalation procedures.

Define the parameters for an escalation well in advance of beginning the project. An escalation raises the awareness and visibility of problems. Having well-defined parameters will help your team decide what issues should be escalated and how to do so. The sooner you know about a problem, the better chance you have of resolving it successfully. If a team member fails to recognize that an issue should be escalated, your project's budget, timeline, or deliverables can be put at risk.

In addition, by clearly defining escalation parameters and procedures, you are less likely to have to defend your decisions later. When you define your escalation procedures and the project sponsor and key stakeholders sign off on them, you minimize the finger pointing that often happens when problems occur.

Documentation Procedures

IT security project plans require a rigorous level of documentation. As you develop your individual security project plan, define the documentation requirements and procedures in detail. It is important to find a balance between the need for documentation and the need to get work accomplished. If you require more paperwork than is reasonable and necessary, the IT staff will likely provide incomplete or inadequate documentation in an effort to get through the tasks quickly. There is nothing more frustrating than performing a 5-minute task and then spending 25 minutes on the paperwork. Be sure you provide IT staff with templates, forms, and easy-to-use procedures to create the necessary project documentation. The easier it is for staff to document the needed data, the more likely they will comply.

One of the real dangers is having staff provide false information because the documentation requirements were too onerous. This could lead to significant security holes, but more importantly, there could be serious legal implications.

You may have more stringent or specific documentation requirements if your organization is trying to become certified or is subject to governmental or industry regulation. Locate the in-house experts on those regulations and be sure to get their input on the documentation needs for the security project plan.

Approval Procedures

Approval procedures should include who approves changes to the security project plan, who approves increases in expenditures, and who approves final deliverables. Create approval procedures that document exactly what is being approved, when it is being approved, and by whom. Keep it clean and simple to ensure that you get the approvals your project needs in order to continue moving forward in a timely manner.

In most companies, the project sponsor is the person who provides the needed approval for most of the changes. Therefore, your approval procedures should specify that all approval points and changes to the budget or schedule must be reviewed by your project sponsor. You should also identify subject matter experts in various areas of security that can be consulted, or you may need to have Human Resources or Legal review certain project parameters before moving forward. Take the time to identify the needed project approval points and identify the person or persons needed to grant approval. When your project is at a critical juncture, you do not want to be running around trying to determine whose signature is needed.

In addition, there are often political and organizational issues surrounding certain types of approvals. For example, if your security project requires a change in the way users access information or in the availability of certain resources (e.g., prohibiting access to secure data outside of normal business hours), you need to determine who has the authority to grant approval for those changes. If you do not go through the proper channels, you may run into an organizational dead end or face unexpected backlash.

Deployment

In the case of IT security plans, there may not be specific deployments or deployment plans required. On the other hand, if you are installing additional security devices such as smart card readers, fingerprint readers, or additional routers, firewalls, or other network hardware/software, you have to develop a deployment plan as part of your security project plan.

The deployment plan should also take into account key stakeholder input; you do not want to interrupt network services during a key client visit or during a major project deliverable. Make sure your deployment plans and associated schedule are known to those that will be impacted by it, so that they can log off. You want to avoid surprise or unplanned disruptions to company operations to the greatest degree possible. The deployment plan should be coupled with pro-active communication plan so that everyone is on the same page (see the "Communication" section earlier in this chapter).

Operations

Another key area in IT security plans is how security will be maintained on a day-to-day basis once you have completed your projects and tightened security. To use an analogy, it does not matter how many locks you have if you leave the door open. As part of your IT security project planning, you should know what is required on an ongoing basis to keep your security measures in place. This includes on-going monitoring, and making necessary changes to ongoing operational activities that reflect the new security policies and procedures. As your business grows and changes, you will have to reassess the impact of that change on your security project plan. If you create a security project plan specifically for performing a security audit, you can use that plan each year (after updating it) to reflect the current status of your company, network, and data resources.

Training

Training runs the gamut from training IT staff on new security software and hardware tools, to learning how to use new tools and techniques for monitoring and responding to attacks, training users how to avoid installing malicious software (malware) on their systems, and so forth. Training also includes training IT staff on new security procedures for ongoing operations. Users often need to be trained, which is another area that your key stakeholder's can help by identifying training needs so that security is maintained throughout the security project plan.

Involve your company's training team in the planning phases and in status reports so they can coordinate their training efforts with your project's progress. Users should be trained as close to actual need for those skills as possible. If you do not have a training department or if this type of training typically falls to someone in the IT department, make sure that identifying training needs, developing training materials, and delivering training programs are all tasks incorporated into your security project plan. Also make sure that the person or persons assigned to these tasks are in the loop regarding project progress so they can plan accordingly.

Finally, there may be training needs along the way. You may think that your team has the skills needed to implement your security project plan, and then find out later that a key member of the team has left the company or is otherwise unavailable. While you cannot plan for these types of possibilities, keep them in the back of your mind as you develop your training outline and your costs for associated training.

Summary

As seen in this chapter, there are some elements of IT security project plans that are different from other projects. Errors and omissions in this area could have a serious impact on your security and, therefore, on your business. Your project team can help you organize your project appropriately, especially if you include key stakeholders in the project organizing process. You may find that you will have different members of the project team on different phases of the project. Identifying and including key stakeholders will help support the project's success. Additionally, stakeholders can provide vital input as to the project's requirements so that the final project plan reflects user, functional, technical, organizational, and regulatory requirements. Once you have identified your requirements, you can create the project's objectives, which describe the project's scope. Finally, organize your project and identify any needed procedures for your security project plan. The necessary planning takes a lot of time on the front end doing, but is a wise investment that will pay dividends on the back end.

Solutions Fast Track

Identifying the IT Security Project Team

☑ A project will be more successful if you involve those outside the IT staff early in the process.

☑ Your IT security project plan team may have different members for the various phases of the project.

☑ Some members of the team may be needed to define and organize the project, a different subset of team members may be needed to test and implement the project, and another team may be responsible for the ongoing maintenance of security after the project is complete.

Identifying IT Security Project Stakeholders

☑ Stakeholders are categorized as involved, influential, and informed.

☑ Involved stakeholders are the people who must be closely involved with the project in order for it to be successful.

☑ Influential stakeholders are those who influence the project. They may not be closely involved in the day-to-day elements of the project, but they will have an influence over the outcome.

☑ Some stakeholders need to be informed. Stakeholders can include the executive team, regional or departmental managers, or the training staff.

Defining IT Security Project Requirements

☑ Taking time to clearly identify the requirements for your IT security project helps you define the scope of your project.

☑ There can be user, Financial, Legal, Accounting, corporate, industry, and governmental requirements.

☑ Stakeholders can be excellent resources for identifying project requirements.

☑ Project planning is an iterative process. You may have to come back to the requirements definition phase after you have done some initial assessments.

Defining IT Security Project Objectives

☑ Projects that are limited in scope have a better chance of success; therefore, defining three to five key objectives per project is optimal.

☑ If you have 10 or 20 objectives, you are probably going into the detail too soon. See if you have any related objectives that can be rolled up into higher-level objectives.

- ☑ If you can only define one or two objectives, your project scope may be too small or you may not clearly understand the problem. If you skipped the problem definition steps (see Chapter 2) or if you short-circuited them, you may want to re-visit them to make sure that you have a clear understanding of your project.

Defining IT Security Project Processes

- ☑ IT security projects require and use defined processes, because omissions and errors can create huge security holes.
- ☑ Keep your procedures simple. Only require as much time, effort, and documentation as is necessary. Unnecessary or cumbersome processes and procedures are almost always circumvented, thus creating potential for error.
- ☑ Each IT security project has different procedure and reporting requirements. Stakeholders can be another source of feedback when looking for checks and balances in this arena.