Chapter 5

Forming the IT Security Project Team

Solutions in this chapter:

- **Identifying IT Security Project Team Requirements**
- **Identifying Staffing Requirements and Constraints**
- **Acquiring the Needed Staff**
- **Forming the IT Security Project Team**

- ☑ **Summary**
- ☑ **Solutions Fast Track**

Introduction

If you're an experienced project manager, you've learned that a security project team makes or breaks a project. A security project plan is nothing but a "to do" list until you have a security project team compiled of competent people who can actually do the work and deliver the results. Therefore, if you don't spend time planning and organizing your security project team, you're missing a huge opportunity, and simultaneously creating a big problem for yourself as project manager. In this chapter, we're going to talk about how to go about forming a security project team for an Information Technology (IT) security project. The material in this chapter intersects with much of the other data presented throughout the book, because the security project team touches all aspects of the project. Even if you're an experienced project manager (which we're assuming you are), you'll gain valuable insight and knowledge from looking at your security project team through the security perspective presented in this chapter.

Identifying IT Security Project Team Requirements

An IT security project team is not a static group of people; its membership should shift and change as you move through the various stages of a project. There will be some people who need to be involved in the initial planning stages to ensure various stakeholder needs are met. However, that same group may not be needed again until the project is in its final stages and you're ready to define standard operating procedures to maintain security in daily operations. Therefore, your first task should be to gather your core IT security project team and define the requirements for that team. There are a number of things that should be considered beyond just who should be involved. Outside of the staffing issue, you should give some consideration to the following areas when forming your IT security project team:

- **Organizational** Which departments, divisions, or sections of the company should be represented on the security project team? Is there a budget issue (e.g., hiring freeze, cutbacks, and so forth) that could impact your project? What about unions or collective bargaining issues that will impact team membership (or the project itself)? Are layoffs imminent or is your company in a hiring mode?
- **Technical** What are the different technical specialties that should be represented on the security project team? Are there different types of technologies (e.g., engineering approaches, software languages, equipment) that should be represented or that will have to be coordinated? What are the technical interfaces that require special knowledge (e.g., database, network, wireless, Web, Virtual Private Network (VPN), e-commerce, and so forth)?
- **Logistical** Where are security project team members located? Are they local, remote, overseas? How will you coordinate their activities? What technologies will you use to facilitate team and project work?
- **Interpersonal** What types of formal and informal relationships exist among team members (or potential team members)? Are there known relationships you can leverage or known issues you can avoid?
- **Political** What alliances exist among various stakeholders and how will these influence your project (for better or for worse)? Are there any people on the IT security project team with political clout, or any members on the team that seem to be out of favor politically? How will this affect your IT project?

Roles and Responsibilities

Once you've reviewed the environmental elements, you should identify the key roles and responsibilities needed for the IT security project team. Do this without regard to the people in your IT department or in your

organization. You need to define an optimal environment first, then you can pare it down to meet both budget and personnel constraints. If you start with a limited view of your staffing needs, you're almost certain to develop a short-sighted plan. Also, if you start thinking of who can fill which role, you may inadvertently have a bias toward (or against) particular people who are currently in certain roles. This, too, would be a mistake. The flip side, however, is that if there is someone in a certain role that you know from past experience (or political savvy) will be a "required" member of your security project team, you'll have to plan around that fact. Sometimes that's a good thing, other times it's a hindrance, but as the security project team manager, you have to deal with these issues.

Roles and responsibilities within your IT security project team are not the same as competencies and staff. Defining roles and responsibilities is independent of who should take them on. People are far more productive when they know what is expected of them and how they fit into the team, so spend time defining these roles. If you need to "borrow" four database administrators for your project, make sure they all understand the role they are expected to play as part of your IT security project team, and that they understand their various roles among themselves. Resist the urge to let them sort it out by themselves, since how they define roles and responsibilities may not map to your needs or your approach. Also, resist the urge to let the person with the biggest title win. One best practice you might want to incorporate into your project management skills is to avoid using organizational titles. If one person comes in as Senior Database Analyst and another comes is as Associate Database Analyst, don't just let the pecking order rule the day. Clearly define how you want these folks to interact, who their lead is, and to whom they all report to in your project structure.

Defining responsibilities typically includes defining deliverables or what each security project team member will be responsible for accomplishing. Again, the more clarity you start with, the better the result.

Working with each member of the team to establish clear, well-defined responsibilities also helps ask and answer questions about conflicting roles, responsibilities, and deliverables. Avoid overlapping responsibilities, and work with the security project team to clarify any issues before getting started on the project work itself. These responsibilities and deliverables also become part of the security project team members' performance review process at project closeout.

To aid in your thinking, we've included a list of roles that might be appropriate to your IT security project. It's not an exhaustive list, but it should help get you started:

- Manager or team lead
- Assistant managers, supervisors, team or group leaders
- Help Desk staff
- Platform specialists
- Trainers
- Support staff
- Technical writers
- Network, System Administrator, and Infrastructure staff
- Programmers and developers
- Web developers and Web staff
- Media and Public Relations
- Marketing and Sales staff
- Legal staff
- Human Resources staff
- Auditors or Quality Assurance staff

Business Intelligence…

Evenly Distributing the Opportunities

We all know that some projects are more interesting to work on than others. Some projects are exciting because they are cutting edge, they use brand new technology, and they have high impact and high visibility. Those are the projects on which reputations can be made. Then there are the mundane, utility projects that have little excitement or interest, but must be done.

As IT manager, you should strive to ensure that even your best performers have to work on some of the boring projects. The only way someone becomes a star performer is to be given opportunities to shine by working on projects with some challenge, visibility, and so on. If you keep allowing your best staff to monopolize the best projects, your junior staff may never get a chance to grow, learn, and show what they're capable of. One way to mitigate the risk of assigning junior members to a high visibility or critical project is to assign a senior team member to oversee the junior team member's work. This accomplishes two key objectives: it mitigates your risk with the junior team member, and it helps develop leadership and management skills in senior team members. Providing these kinds of growth opportunities in a controlled and manageable manner is part of what makes people enjoy their work. Most people are far more satisfied working in an environment that leverages their talents and provides opportunities for growth.

Competencies

In addition to identifying roles and responsibilities, your IT security project plan will undoubtedly require very specific sets of competencies. Again, avoid thinking about specific people at this point, and work to identify the competencies required. This is one area that will probably require some revision down the road (e.g., your corporate IT security project plan will include several Individual Security Area Projects (ISAPs), and those ISAP's may each contain very specialized competencies. You

want someone very familiar with Intrusion Prevention Systems and Intrusion Detection Systems (IPS/IDS) to implement your IPS/IDS solution, and you want someone very familiar with your database structure and use to help design and implement a database security solution). These are competencies you can identify generically as you go through your planning process and develop additional detail as it becomes available.

Keep in mind that competencies are not confined to technical competencies. You should consider including competencies from other areas such as:

- Technical
- Communication (verbal and written)
- Training
- Negotiation
- Translating technical language into user language
- Reporting
- Legal, financial, regulatory

Technical

Obviously, your competencies list would not be complete without a full list of the required technical competencies as a starting point. Though you've probably got this covered, it is wise to sit down and review which technical competencies are required for all of your IT security projects (i.e., the corporate IT security plan and the ISAPs). This may be a list you have to re-visit a few times as your IT security project plans come into focus. Creating this list of required technical competencies can help you determine if you have the expertise in-house, if you need to train internal staff, if you need to hire additional staff, or if you need to hire an external vendor. Knowing where your technical competencies are and where your gaps are will help you create a viable staffing plan. Having untrained or

unknowledgeable (or outright incompetent) staff performing critical or complex technical security tasks can leave gaping holes in your security systems.

Communication

Let's face it. IT departments are not known for their wonderful communications skills. Unfortunately, many IT departments do a terrible job communicating, probably because the IT staff are so busy working on technical issues that they forget (or try to forget) there are users out there awaiting information, responses, and updates. When putting together your IT security project team, look for one or more people who are good at communicating and enjoy it. You may have to look for someone outside your department to help, by having them attend key meetings and write up brief status updates and announcements on behalf of your security project team. That's fine, as long as you make communicating with key stakeholders a deliverable in your security project plan. Remember, project success is as dependent on *perceived* success as it is on *actual* success (perceived success, in fact, trumps actual results). Therefore, it is very important to find someone who is good at communicating, who can add communication tasks to the security project plan and be the task owner and implement those plans.

Training

Training is another competency you should have represented on your security project team. Someone with a training background or perspective can help identify areas that will require IT staff training and user training. Including this competency also creates awareness of the need for training, and can help ensure that training tasks are either included in the security project plan or are appropriately tied in with the security project plan through the Training and Development department.

Negotiation

You may not think that negotiation is a necessary competency for an IT security project team, but it can be helpful to have, especially when you have to negotiate a bigger budget, the loan of several key staff people for a months-long security project team, or with a vendor for a large security-related purchase. Negotiation is how business gets done, and if you have someone on your security project team that is comfortable (and successful) at negotiating, it can help your project tremendously. Keep in mind, however, that not everyone approaches negotiating in a similar manner. In some respects, it's very cultural (country-to-country, company-to-company, department-to-department, individual-to-individual). Ensure that if you bring someone to the security project team to help negotiate, that he or she has similar values to you and your team. If the negotiator believes in "winning at any cost" and your attitude is "create a win-win outcome," you're likely to get a result from your negotiator that you don't like. Set clear rules and boundaries if you have someone else negotiate on your (or your team's) behalf.

Translating Technical Language

IT people sometimes forget how to say things in plain English. Rather than explain that the server requires Simple Mail Transfer Protocol (SMTP) server authentication and that you'll be implementing Secure Password Authentication (SPA), they simply tell the user that they'd be securing outgoing email. The ability to translate technical language and jargon into plain English (or some other language) is a competency that is sometimes under-represented on IT teams. By explaining things simply and clearly, and in an appropriate (e.g., not condescending or simple-minded) manner, you can help users and executives become more comfortable with what's going on behind the scenes. Remember that most executives and users think IT is spooky, secret stuff. By translating it for "normal" people, your IT project details can be more accessible and therefore less threatening.

Reporting

Have you ever noticed how some people have a knack for coming up with perfect report formats? They seem to instinctively know what data belongs together, how it should be organized, and how one piece of data relates to another. These folks can be valuable assets to a security project team, so you may want to include reporting as a competency. Having one or more security project team members with this ability can help you develop meaningful reporting procedures. Various stakeholders require different types and frequencies of reporting. You could have a security project team member with a strength in reporting plan the various types of reports. This can contribute significantly to perceived project success, since most people are satisfied with accurate, timely information.

Legal, Financial, and Regulatory

When you're dealing with an IT security project plan, you have to make sure that your legal, financial, and regulatory bases are covered. Identifying the competencies needed for your IT security project(s) and including them in your security project plan, will help ensure that you pull in the right professionals at the right time, and that you leave no gaps in your security project plan.

Once you've created the list of competencies (some may be required, and some may be optional that could enhance the project), you can begin laying out a rough timeline for when those competencies will be needed (e.g., you might find that you'll need the Legal department to review the regulatory requirements and translate them into plain language at the outset of the project.) You may not need the Legal department again for your security project plan, or you may need it to advise the Human Resources department on the implications of performing employee background checks on all employees who will have access to Research & Development (R&D) data. If you can identify when during the project lifecycle you're likely to require these various competencies, you will have a head start on your staffing requirements and staffing plan.

There may be additional competencies not listed here that your IT security project plan will require. This is a good time to give it some serious thought, and to get your security project team to think the project through to help identify needed competencies. The more thought you give to it now, the less it will keep you up at night.

Identifying Staffing Requirements and Constraints

Once you've identified your required competencies, you have to begin looking at your staffing requirements, which match competencies with actual people in (or outside of) your organization. Look for the optimal candidates for each competency first, and then make note of the second, third, and fourth choices. Devise strategies for filling gaps, either through training, hiring, or contracting. In some cases, it may be appropriate to divide your IT security project plans into phases and shift your competencies accordingly. Sometimes you can reasonably delay hiring or training until a later phase.

Reality usually sets in once you've created your "dream team" (e.g., Jill is temporarily on assignment in Madrid, Spain; Craig is your best IPS/IDS guy, but he's out with a family situation for another month; John is your go-to guy for all Internet-related work, but he's already working overtime to get the new Web site up and running; Lisa is absolutely your best security administrator [users, access controls, auditing, log file management, and so forth], but she's recently been promoted and will be heading off to a new position at a regional office within the month.) You know the drill; your best people are not always available and yet you have a project to plan, implement, manage, and complete. Determining your staffing constraints is where you insert a bit of organizational reality into your "perfect world" security project plan, so that you can actually get your project work done.

Sometimes your staffing constraints are financial. You may need four database administrators to help design and implement database security, but you'd have to temporarily transfer them to your IT payroll and your

budget doesn't have the room. Other times you may need to hire a contractor with a specific skill set or hire a new position or bring in a security consultant—all while you're being tasked with improving security for about 5 percent of your overall IT budget. While life and budgets aren't always fair, your job as IT security project manager is to find creative solutions to these problems. Brainstorm with your security project team or make a strong business case to your security project plan sponsor. Whatever you do, you'll have to live with staffing constraints and negotiate your way through the process.

This might also be a milestone or checkpoint that you can use to sit down with your security project plan sponsor and discuss your staffing needs. Since most company's budgets are not unlimited, you're probably going to have to make a few tough decisions. Best practices include going to your security project plan sponsor prepared with your staffing needs, costs, and alternatives. Don't march in with a list of demands, and don't expect your sponsor to solve your problems for you. Be prepared, and come in with various alternatives along with the risks and rewards of those alternatives. Work cooperatively and proactively with your security project plan sponsor to find acceptable solutions to the staffing and budget limitations that you might encounter.

Also keep in mind that if you cannot gather the people you need to fill critical (or required) roles or to provide required competencies, your project is at risk of failing. Though you haven't moved beyond the planning stage yet, you will be positioning your project to fail if you take off without adequate resources and simply hope that something will change down the line. As much as you might not like being the bearer of bad news, you have to work hard with your security project plan sponsor to find a reasonable solution. If your sponsor "orders" you to proceed despite your lack of critical resources, you will have a serious problem on your hands for two reasons. First, it will spell disaster for most projects and, second, you will have a serious security problem in the making. If you can't find someone competent enough to install or configure a new IDS system, you could potentially open the floodgates for hackers—not a good situation and one that will absolutely come back and fall on your

shoulders. This can be a difficult situation, but unless you're going to get fired for saying, "I don't want to proceed until I have the needed resources for success," hold firm and negotiate for what you need. Don't hold a hard line—get creative, be flexible, and find the necessary middle ground to get your security project plan work accomplished successfully. The goal is to increase security from its existing state and to find out whether or not you have the right resources to help you get there.

Acquiring the Needed Staff

Once you've determined who you need and when, you'll need to put some thought into how you will actually "acquire" those people for your security project plan. Some companies have very formal procedures that must be followed, that track time, expense, department, and project numbers. In other companies, it's a negotiated process (e.g., "You need Justin? You can have him two hours a day for the next month. I can't afford to have him away from his other work any more than that."). Be sure to talk with the person's direct supervisor or manager to get the okay first. No one likes their staff yanked out from under them (or enticed onto a project with promises of fame and glory), so be sure to use common courtesy when gathering your security project team. In addition, there may be something about Justin's performance that you don't know. Suppose Justin has just been put on a performance improvement plan because he's been spending most of his days surfing the Internet, and not getting much work done? Suppose Justin really is an incredibly bright guy, but doesn't get along well with others? Do you really want him on your security project team? The flip side is that you should try to ensure that the people you think you want on the team will actually be valuable members. You can ask others who they'd recommend for a particular role or to provide a particular competency, to see whose name keeps popping up. If Justin's name never comes up, it should make you wonder if he has trouble working well with others, doesn't carry his weight, talks incessantly, or has some other behavior that causes people to avoid working with him.

Beyond that, you'll need to think about some of the routine aspects of managing a team, including:

- Where will the team meet and work?
- What procedure is needed to formally pull someone onto the project?
- What cost accounting procedures are required to track personnel costs?
- How are external staff (vendors, contractors, other departmental staff) acquired and managed?
- How you will handle staffing if project timelines slip?

At this stage of your IT security project plan, you may not have enough detail to answer these questions; however, they should be answered at some point. Project management is an iterative process, so you will likely have to review these questions periodically as you plan and implement your security project plans.

Forming the IT Security Project Team

Your IT security project team will likely require a rotating or changing cast of characters, so you may want to name your various teams (e.g., a "project definition" team, a "requirements" team, a "communications" team, a "training team," and so forth). There may be some people who are members of several teams and others who are members of only one team. If you want to get creative and have fun, you can let the teams name themselves around a common theme (so there's some relation and they can be easily remembered). Once your teams are formed, your first step is to create team rosters. This will help the team members know who's on the team and how to contact other team members. It will also help you as you move through your various projects, since some teams won't fire up until later in the project lifecycle.

Identify Training Needs

At this point, you'll also need to identify your initial training needs. You have already identified your project's required competencies and the people needed to provide those competencies. However, if your company is like most, you have a few gaps between the needed competencies and the available staff. Determine if you need to provide training to fill those gaps.

Whether you provide training or hire external consultants, contractors, or vendors, you'll need to make sure there's room in your project budget for these additional costs. These are the kinds of costs that often sneak up on you and cause you to blow your project budget even before the project has gotten underway. This is another checkpoint between you and your security project plan sponsor that you can use to perhaps shift some of the training costs to the Training department or the Human Resources department (if appropriate), or to ask for additional funds specifically earmarked for training.

Team Processes and Procedures

If you're an experienced IT project manager, you probably have a hard drive folder or notebook full of project processes and procedures that you've developed over time. If so, this is the time to pull them out and review which ones you'll need, and which ones that may need to be modified to meet the needs of this particular project. We've provided a refresher list for you, but if you need a more thorough review, go back through your IT project management documents to make sure you've covered all the bases.

- How often will security project team meetings occur?
- Where will they be held?
- Who must attend?
- How long will they last?
- How should team members prepare for these meetings?

- How will the meetings be facilitated and what is expected of the participants?
- How will status be reported to you? How often and in what format?
- How will project status be reported to executives, users, and other stakeholders?
- How will project performance be tracked, measured, and assessed?
- How will project team members' performance be tracked, measured, and assessed?
- How will problems be handled?
- When will problems be escalated and resolved?
- How are project changes made?
- How are project change requests evaluated, implemented, and tracked?
- What type of documentation are team members expected to keep?
- How and where is project data captured and archived?
- *How will security checkpoints or milestones be identified, verified, and documented?*

Though this list is fairly long, it covers the essentials. The last bullet point is in italics to specifically highlight that particular issue. Project processes for standard IT projects work fine to a point. However, you also need to look at processes and procedures that will document your security improvements, especially if you are subject to various regulatory or legal requirements. The problem with some of these requirements is that they are vague or unclear, and they leave organizations with a lot of questions about exactly how to implement them. While the legal authorities are sorting it all out, you can attempt to make sure your bases are covered by developing processes and procedures for documenting

everything (including your documentation) so that you have the needed data at hand.

Your security project may require other very specific processes. However, make sure that any and all processes and procedures you introduce actually help drive the project forward. Some people mistake *process* for *product*, meaning they think that all of the busy work associated with developing processes and ensuring people comply with the processes actually accomplishes security project plan work. In fact, processes and procedures that are overly burdensome will grind your project to a halt. Check with your security project team about what processes and procedures will help them get their jobs done. If you believe additional processes are required, check with the team to ensure they'll actually help. Process for process's sake is just a waste of time.

Team Kick-off Meeting

At the beginning of the project, you should schedule a security project team kick-off meeting that includes all members of the team. You may choose to include those who will participate in the project in later phases, in order to create a cohesive team and to provide a sense of starting off together. Planning this meeting (and subsequent team meetings) will help it be both interesting and productive. The security project team kick-off meeting is the first and best opportunity to get people excited about the project, and to assist them in forming the necessary team relationships that will help the project move forward. A solid foundation for the security project team will weather any bumps in the road that may occur later on.

Keep in mind that an effective meeting is one that has a specific purpose. We have all attended meetings that wandered around and at the end of the allotted time, nothing was accomplished. If you want people to attend your meetings, make them so action-packed and useful that no one wants to *miss* one. Clearly state the purpose of the meeting in the invitation. Attach or later forward a meeting agenda with clearly defined objectives and outcomes. Start and end the meeting on time, actively manage the meeting, move it along, and keep the conversation on topic.

Assign action items for follow up along with due dates and owners. If meetings are productive, your team will attend. If meetings are a waste of their time, they'll find excuses not to attend and security project work will often begin to fall behind schedule.

The team kick-off meeting sets the tone. You can start your project off on the right foot by holding an effective meeting with your new team.

Business Intelligence…

Geography and Project Teams

We all know that IT security project teams can be (and often are) geographically dispersed around a country or around the globe. If you're managing a security project team that is not centrally located, your communication skills are even more important. If you're managing a global team, you have your work cut out for you, especially if you don't have existing relationships with some of your team members. Keep in mind that people in different countries and cultures communicate differently, they approach work differently, they interact differently, and they respond differently to feedback, criticism, and debate. If you are managing a global team for the first time, you should make a concerted effort to understand the culture from which your team members come and how they view work and their participation on the team. Remember, too, that security may be viewed very differently from one country to the next. Finally, keep in mind that terminology should be well-defined; you should check for understanding before assuming everyone is on the same page. While technological terms are somewhat "universal" in nature, be sure that everyone has the same understanding—whether they're across town or across the globe.

If you're looking for a few communication tools that work with worldwide teams, consider instant messaging, email, Skype, Voice Over Internet Protocol (VoIP), and any one of the variety of online collaboration tools such as *GoToMeeting.com*, *WebEx.com*, *LiveMeeting.com*, or *Windows NetMeeting* (or many others) in order to collaborate in as near real-time as possible.

Summary

Forming the security project team is one of the most important planning tasks, because projects don't just run themselves and project tasks don't just magically get done—they rely on people to do them. Therefore, the people you surround yourself with on this project will be the key to success. Taking time to start at the top and define the roles, responsibilities, and competencies needed will help you avoid narrowing your focus too early. Often if we like or dislike someone with a particular skill or competency, our decision making can be influenced. Starting with the impersonal data will help ensure you create a solid list before focusing in on the specific people you need.

Since there are few companies where people are just sitting around waiting for their next assignment, you will have to contend with a variety of staffing issues and constraints. How they manifest will vary from company to company; you're probably well aware of the issues you're likely to face. This is a good time to sit down and talk with your project sponsor to make sure you have his or her support and to help you gain the resources you need to ensure a successful project. If you are unable to secure the necessary people (skills, competencies, roles) for your project, you're headed for a very rocky road ahead. Be flexible and creative when looking for ways to resolve staffing constraints, but don't launch a project with glaring staffing holes either.

Define project processes and procedures from A to Z so your team can get its work done quickly and efficiently. They should know how, when, and to whom to submit a status report and what data should be in that report. They should know how to notify the team or you of a problem, and how to escalate and resolve problems. They should understand what constitutes a change, how to submit a change request, and what the procedures are for managing change requests throughout the project lifecycle. Processes and procedures help the project run smoothly and they help you avoid having to reinvent the wheel from project to project.

Solutions Fast Track

Identifying IT Security Project Team Requirements

- ☑ Organizational, technical, logistical, interpersonal, and political requirements should be considered when forming your security project team.
- ☑ Roles and responsibilities should be identified for the security project team, to help everyone form a clear picture of where and how they fit in.
- ☑ Competencies should be defined without regard to which specific person or people will provide those competencies. Start with your ideal "wish list" and pare it down, as needed.
- ☑ Competencies can include (but are not limited to) technical, communication (verbal and written), training, negotiation, translating technical language into user language, reporting, legal, financial, and regulatory.

Identifying Staffing Requirements and Constraints

- ☑ Once you've identified the skills and competencies you need for your security project team, you can begin identifying people to fill roles or to provide specific competencies.
- ☑ You may find that you have roles or competencies required for the project that you cannot fill with company resources. You'll have to devise a plan for obtaining the necessary resources you need, and check with your security project plan sponsor.
- ☑ Staffing is always influenced by various constraints, from vacation time to other company obligations, to politics and beyond. Your job as project manager is to make sure you have the resources you need to deliver a quality IT security project.

- ☑ If the quality of your project will be significantly impacted by staffing constraints, you should work closely with your security project plan sponsor to address those deficiencies. Moving forward as if resources will magically appear or problems will disappear is unwise.

Acquiring Needed Staff

- ☑ Give some thought to how you will actually "acquire" the staff you need for your security project team. Consider your company's culture, organizational style, and staffing levels.
- ☑ Make a practice of talking to a person's supervisor or manager before talking directly to a staff person you'd like to join your security project team. It's polite and may save you problems later on.
- ☑ Ask around to find out who other people would recommend for a particular role or to provide a specific competency. This gives you a clue as to how others view individuals within the organization. If someone is very smart but impossible to work with, you might think twice about inviting him or her to the security project team if you have other options.

Forming The IT Security Project Team

- ☑ As soon as you know who the members of your security project team are, create a team roster. This provides everyone a list of team members and contact information and begins to create a sense of belonging to a team.
- ☑ You may create several sub-teams and provide sub-team rosters for those participating later in the project lifecycle or those participating on a particular section of the project.

- ☑ Once you've put your security project team together, you should look at their training needs. It's more common than not that you were unable to get your "dream team" and some skills gaps may exist. Addressing training needs at the outset will help you plan and budget appropriately.
- ☑ This is also a good point to define security project team processes and procedures. You may have a fairly standard list of these that you can reuse, or you may have to define new ones just for this project. A thorough set of processes and procedures helps team members be more productive with less effort.
- ☑ Remember that security-related processes and procedures, especially those required by law or other regulation, should be built into your security project planning process.
- ☑ Be sure to plan a security project team kick-off meeting, so that you can begin to create a sense of the team and let everyone know that the project is underway.