Chapter 8

Closing Out the IT Security Project

Solutions in this chapter:

- **Evaluating Project Completion**
- **Closing Issues Log, Change Requests, and Error Reports**
- **Preparing for Implementation, Deployment, and Operational Transfer**
- **Reviewing Lessons Learned**
- **Documentation and Compliance Reports**

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

Introduction

In previous chapters, we focused on the elements of Information Technology (IT) project management that are particular to a security project plan. This chapter focuses on standard project management methods. (For the purposes of this chapter, we will assume that you have a solid IT project management background.)

Closing out a security project plan is different from closing out a standard IT project plan, because there are more serious ramifications for security projects. In a standard IT project, if you change the scope, decide to forego a few tasks, or are unable to resolve a problem, you can usually save those issues for a subsequent project or version. In the case of security, what you skip over or omit could be what hackers find and exploit; therefore, the project close-out process must be thorough and diligent. In this chapter, we look at determining when the project is complete, how to close out various issues, and how to prepare for implementation, deployment, and transfer. These elements are critical to maintaining security; thus, particular attention must be paid to this area. Finally, we look at capturing lessons learned and finalizing project documentation. This is another area that may require a different approach than that of a standard IT project, due to the potential for compliance with various laws, regulations, or standards related to network and data security.

Evaluating Project Completion

When is your IT security project complete and how will you know? The obvious answer is, "When all tasks are 100 percent complete," but a more accurate answer might be, "When all tasks on the critical path are 100 percent complete." Still, that's not a real-world answer, because the actual data vs. the planned data are often at odds with one another. As you near the conclusion of your IT security project plan, you should begin gathering data, status reports, and other information that will help you determine exactly when your security project plan will conclude.

There are numerous project tracking methods you can use for your IT security project to determine actual project completion. If your project parameters specify that the budget (cost) is the priority, you may have to terminate your project when you reach a specified budget amount, regardless of whether or not you've completed the project tasks. By the same measure, if you determine that schedule (time) is the highest priority, you may have to terminate your project when you reach a specified date or deadline, even if all of the project tasks have not been successfully completed.

The problem with this is that if you fail to complete all project tasks, you may be leaving yourself open to security breaches. As you manage the project, you need to keep these parameters in mind. You may have to make a few tough decisions (e.g., omitting a particular set of project tasks after determining they are not needed immediately or can be postponed with minimal risk). With security, you fall into a difficult situation where you can't reasonably reduce the scope, increase the budget, or lengthen the schedule without putting the security at risk. Some of the tasks that could potentially be omitted or delayed from the current project might include upgrading a particular technology that meets specifications today, but is not optimized for handling evolving threats. You might choose to delay this until a later phase when time, money, or resources are more available. This is not without risk to overall security and the project itself, but is an example of the kinds of situations where you might have to make a difficult trade off.

If you find yourself approaching the end of your schedule or the bottom of your budget and you haven't completed the security project plan, you have a problem. In Chapter 7, we recommended you keep your project parameters in the forefront of your decision-making, and that you actively manage the scope to avoid running into these problems. While problems will inevitably arise, managing them pro-actively will help you avoid running out of leeway on your project.

When all is said and done, it's a good idea to step back and look at the actual data vs. the planned data to determine what worked, what didn't work very well, what went horribly wrong, what snuck up on you,

and what worked surprisingly well. In every project, there are all of these elements and looking at your project in retrospect will help you and your team learn a lot about many aspects of the project, the organization, and the team. A project summary report is often required (or desired), and the opportunity to look back through the report should be utilized in a positive, productive manner. Some company cultures seem to get locked on the negative aspects, and project reviews turn into blame-fests. Don't let this occur. Look at what worked, what didn't work, and what can be improved for next time. Be brutally honest in your review, but be professional and positive in your communication. Create a culture where people feel comfortable admitting their shortcomings, errors, or omissions so that a better system can be created to avoid those problems in the future. If you create a culture where people are reluctant to identify or own these issues, they'll keep cropping up. Remember the saying, "The definition of insanity is doing the same thing over and over and expecting different results."

Closing Issues Log, Change Requests, and Error Reports

As with any IT project, issues logs should be actively managed throughout the project lifecycle. If you've assigned an owner of the issues log (see Chapter 7), you should have little problem with outstanding issues at the end of the security project plan. If you have not been actively managing the issues log, you run the risk of ending up with open issues that prevent project closure or leave a huge security hole. Issues log items should be resolved and the resolution should be well-documented. Also, you may have legal liabilities that stem from the issues and resolutions (see Chapter 7). Addressing known issues in a reasonable manner and documenting those resolutions are important elements of reducing risk.

At this point in the process, change requests should be addressed and resolved. These change requests should be recorded, evaluated, incorporated (or rejected), and documented. As with issues, the key in an IT security project plan is to thoroughly document the changes made so you can

update your documentation, operational procedures, and policies. At project close-out, you should not have any open change requests. Change requests should be evaluated and incorporated into the security project plan task plan or they should be rejected. If any are still open at the end of your project, it's usually because you have changes that need to be made to something that falls outside the scope of the project. If this is the case, be sure you find an appropriate method for transferring this knowledge to the appropriate parties (e.g., a change request deemed to be outside the scope of the project might be transferred to the training department so they can develop targeted training on this topic for users). Rather than changing the project itself, you might decide that changing a user procedure or policy makes more sense and delivers the same or more security.

Typically, error reports indicate a problem that should be resolved before a project is closed out. However, in some cases, error reports fall outside the scope of the IT security project plan. When this happens, the team decides whether the issues can be resolved in an alternate manner. An error report outside the scope of the project should be tracked as an "issue" that can be transferred outside the project during close out. If it's an actual error, it should be resolved within the scope of the project.

The net result is that all issues, change requests, and errors should be resolved or transferred at project close out. Whatever process you use, document all of it so you don't get caught short during an audit or in the aftermath of a subsequent security breach. Also, a security project has more legal and regulatory implications.

Preparing for Implementation, Deployment, and Operational Transfer

We've already covered closing out the issues, change requests, and error logs and transferring any open or outstanding items to the appropriate places. Beyond closing these items out, you should begin looking at the other elements of the IT security project that need to be documented and handed-off for implementation, deployment, or operations. Many of these are standard processes you've used countless times in other IT pro-

jects; however, when you move into the realm of IT security, there may be additional steps needed to complete the preparation for project completion. Remember, too, that since the perception of project success is as important as real deliverables in the minds of many stakeholders, how you handle closing the project and transferring operational knowledge can increase or decrease that perception. Users and others in the organization may only see the operational component, since much of the project plan may be done by subject matter experts including security analysts and high-end IT staff. Therefore, how you handle this aspect of the project may be the only part visible to the organization and may be the only thing upon which success is judged by a majority of stakeholders. Of course, at the end of the day, project success will be tied to what *doesn't* happen (e.g., the intrusion averted, the data secured, and so on). As we've discussed, it's often hard to tout success based on the absence of something, so your most tangible opportunity to tout project success may be through this operational transfer process. Make good use of it.

Preparing for Implementation

Implementing security elements is often part of the IT security project plan. However, there may be instances where certain portions of implementation fall outside the security project plan. This might include changes to policies and procedures that are recommended but not implemented, or changes to logons or other security methods that must be rolled out in a particular manner or in a particular timeline (e.g., some companies might choose to implement security measures in segments, such as first implementing security measures for all users in the Finance department). This is often done to find and resolve problems that may arise during the implementation phase without completely disrupting the organization. Your security project plan may have other kinds of implementation needs that will be completed outside the security project plan itself, or after project work is complete. If implementation happens outside the scope of your security project plan, be sure that the information required for implementation is well-developed by defining the imple-

mentation requirements and including tasks that address implementation needs. Also, be sure to include milestones in your security project plan so that internal (to the project) and external events remain in sync. Finally, be aware of the need to review your implementation plans from a security viewpoint. If you're implementing changes outside the scope of the project, are there risks to doing so? How will you test, monitor, and remediate implementation results? Who is responsible for the implementation work? Keep these issues in mind as you begin to close out the project, so that all of your hard work on the security project plan is supported throughout the implementation plans.

Preparing for Deployment

Deployment might also be part of the IT security project or it might fall outside the scope of the security project plan. Deployment might include installing new Intrusion Detection System (IDS)/Intrusion Prevention System (IPS) systems or upgrading servers based on recommendations from the security project plan. Security project plans often include the deployment of security solutions as a second phase of the project, but this varies from company to company and from one IT security project plan to another. Deployment includes installing hardware and software and documenting how they will be installed, tested, and turned over. In some cases, this is the same as an implementation plan. In other projects, there is a discrete deployment team whose job it is to take the recommendations and deploy them. As with an implementation plan, a deployment plan that is outside the scope of the security project needs to tie in closely. The deployment team needs to be aware of the security project plan timelines so they can plan accordingly. They also need to be aware of problems, issues, and questions that are still open so they can either participate in solving/closing those issues or so they can work around them.

All deployment plans should include a rollback plan that explains what you should do if things go wrong. Delineating the steps for backing out of a security implementation or deployment is important especially if the deployment causes significant network or resource access issues. If

someone sets access control to critical files on a database server incorrectly and no one can access these files, what steps will you take to quickly resolve this? What if these changes have already been replicated across the enterprise? These are the kinds of things you should include in your deployment rollback plans for the major changes you're undertaking. Identifying how to roll back to the last known good state is an important part of the planning process, especially if these plans follow your IT security project plan.

Preparing for Operational Transfer

Operational transfer typically refers to the point at which a project is handed off to the users. However, in an IT security project plan, this may also be transferred to the IT staff responsible for the day-to-day operations. Since your security project plan(s) may have utilized subject matter experts to assess security and develop security solutions, your project may have developed information that needs to be documented and transferred to whoever is responsible for the day-to-day operations. In essence, the operational plan should include:

- The tasks for handing off the project deliverables
- The strategy to be used for the handoff (How will the handoff occur?)
- The key resources needed
- The task owners
- The timing of transfer tasks
- The cost of transfer tasks
- The schedule for transfers
- The risks and contingency plans for transfers
- The formal acceptance or closure methods for transfers

Your IT security project plan concludes with a successful transfer to operations. These operational plans form the keystone to maintaining security and, in particular, maintaining compliance after the project concludes. Therefore, it is critical that sound planning occurs at this juncture. These activities can be included in your IT security project plan itself, or they can be a separate implementation plan, whatever works best for your situation. Keep in mind that you should document operational issues throughout the project lifecycle, so that when it comes time to transfer operations you have well-documented data. Your operations data should include procedures for:

- Maintaining new security measures
- Monitoring security
- Reviewing and analyzing security audit and log files
- Taking action based on audit and log file analysis
- Alerting an emergency response team to a potential security problem
- Addressing user issues with new security policies and procedures
- Escalating emergency and ongoing issues
- Ongoing user security awareness and education

Be sure you identify the timelines for transfer and provide all necessary training, information, and documentation, so that the hard work undertaken during your security project plan lifecycle will be supported, maintained, and perhaps enhanced.

Business Intelligence…

Don't Just Lob It Over the Fence

Operational transfer is a critical component to maintaining IT security, even though some of these areas can fall outside the normal domain of the IT department. IT may not be involved with developing user policies beyond some basic IT issues like password complexity; however, in the world of IT security, paying close attention to operational transfer is very important. If you drop the ball here, all of that hard work you and your team did during the project lifecycle is put at risk, because all the best security measures in the world don't add up to anything without consistent operational security afterward. Operational transfer often hands over control from the project team to the user, but in the case of IT security, it might also include transferring operations from the project team to the IT staff who manage day-to-day operations. In either case, be sure that your project deliverables include the details and necessary information for the operations team. If necessary, create several working sessions where the project team can do a download to the operations group and provide the detailed information necessary for a successful hand off.

Reviewing Lessons Learned

As mentioned in Chapter 6, it's a good idea to document lessons learned during the course of the project itself, rather than wait until the last minute to gather this data. This should be included in the task details and the information should be shared with the team during the course of the security project plan. It's often the case that lessons learned can be used during the remaining project plan. At the end of the project, however, you should have a wrap-up meeting to review the lessons learned, the context of the lessons learned, the improvements that can be made, and the positive things that worked and should be repeated in the future. While it's important to discuss tough issues head on, it's also important to

focus on what worked well or what you discovered that you could use in the future to make subsequent projects more successful.

Some of the things you should have captured during the project include:

- Problems resulting from incomplete or unclear project definitions (problem, mission, potential solutions, selected solution, project priorities).

  Example: The lesson learned might include spending more time defining the specific problem so that the project is more targeted or focused. It might also include spending more time with stakeholders in advance of project planning. Finally, it might involve asking someone from human resources to facilitate your planning meetings so they are more productive.

- Problems arising from lack of clarity or agreement regarding project parameters including scope, schedule, budget, and quality as well as the relative priority of each of these factors.

  Example: Users will be able to logon to access files. If a metric measures project success, it must be specific and measurable. Users will be able to logon to the system with a single username and password to access files across all domains. The logon should be completed by the server within 10 seconds of user data being submitted locally. Users logging in via remote connections should receive authentication within 20 seconds, depending on the user's connection speed.

- Problems arising from inaccurate or unrealistic scheduling or budgeting.

NOTE

Scheduling and budgeting are skills that are improved with practice and evaluation. Being honest about how well you and your team did in this area will help you find ways to improve for future projects).

Example: It is not possible to develop an accurate schedule until the requirements are clearly understood. One solution is to revise the high-level project plan and the high-level schedule in more detail as the project becomes more defined. This allows you to know if the project is getting too expensive. Too often, initial estimates are used as targets; learning to refine estimates and manage expectations is often a lesson learned in project management.

- Changes to the scope that caused problems including how changes were requested, evaluated, implemented, and documented.

  Example: Your current change management process may utilize a monthly change request meeting, but changes are occurring in the project that have not been discussed in the meeting. You may need to revise your process to include a more formal, written acceptance of changes so that stakeholders are not slipping changes in through back channels.

- Problems resulting from organizational challenges including lack of executive support, lack of organizational support, lack of reporting clarity, lack of resources stemming from organizational constraints, unanticipated organizational change, and so on.

  Example: You began implementing security changes for remote access, but the marketing department put an immediate halt to the security project plan because they were in the middle of a huge client project. Their plan was being disrupted in ways no one anticipated, and they could not afford the downtime. The lessons learned here might include bringing in a wider group of stakeholders during the planning process, and communicating more effectively about the expected outages and timelines once the security project plan begins, so that any mission-critical activities can be accommodated.

- Things that were unplanned and unanticipated that disrupted the project.

- Anything that worked well (as opposed to a problem) from Items 1 through 6 above.

  Example: Two Finance department employees and two subject matter experts assisted you in developing a more refined project budget.

Sometimes lessons learned are much simpler than that. It might be that someone discovers a faster, easier method of updating server settings or restoring a security template. It doesn't have to be a major, life-altering change to be worthy of mention. You may choose to create two categories—one called "Best Practices" and the other one called "Lessons Learned." In this way, you can differentiate between the two and share the data accordingly.

Whatever you do, make sure you don't just gather the data, record it someplace, and move on. If you never incorporate the information, you've wasted your time capturing it. Find ways to make use of the data so that you and your team can continuously hone your project management skills and make continuous improvements. In this rapidly changing global business environment, organizations that don't learn often fail. This is a great opportunity for you to help ensure your organization continues to grow and learn and remain competitive in a highly competitive world.

Documentation and Compliance Reports

Documentation for your IT security project comes in two basic flavors: documentation you and your team need for departmental or organizational reporting, and documentation you need for regulatory compliance reports. These are not necessarily one and the same, although to the extent that you can re-purpose material or generate one report that will serve two purposes, you'll be better off. Finding ways to streamline reporting and documentation from a compliance perspective is important, and you may choose to purchase a software solution that helps you main-

tain security and compliance. This may be part of your overall corporate IT security project plan or it may be a task or a sub-project.

The specific data needed to document your project at close out will vary depending on the details of the project. At minimum, you should have the following:

- Status reports from your team.
- Project status reports to your executive team.
- Project status reports to your project sponsor.
- Original project plan (including work breakdown structure [WBS], schedule, and budget).
- Revised project plan (including any change requests that were incorporated).
- Final project plan (including final schedule and budget).
- Lessons learned and best practices.
- Project team member performance reviews (some companies do this as part of project close out, some do not). Follow your company's practices regarding this or check with your Human Resources department).
- Suggested or implemented revisions to standard operating procedures.
- Suggested or implemented revisions to company and user policies and procedures.
- Documentation for user training (if applicable).

Let's look at these in more detail. The status reports from your IT project team should be collected and archived in some accessible location in the event there are any questions about what was done when. Again, these may end up as legal documents, so they should be handled in a manner appropriate to your company and the regulations under which it operates. If in doubt, seek the appropriate legal counsel. In some cases,

these documents can raise more questions than they answer—especially if they are informal documents—so, be sure to either dispose of them or archive them in a manner appropriate to your situation. The same holds true of status reports to your executive team or project sponsor.

The original security project plan, including the WBS and all defined tasks, should be archived for two reasons. First, it's good to have a copy of the original plans for future reference. You will want a snapshot of the project in its original state for review and assessment. Second, the original project security plan details the scope of the project and may be used (or needed) later to assert that your firm took "reasonable care" to address security issues. This is a two-edged sword, however, since you may also find that your final project plan was scaled down and that one or more fairly important security areas were left out of the security project plan due to financial or scheduling constraints.

You should also review the original project documents against the final documents. In particular, review the actual data vs. the planned data for major tasks or deliverables, to see how well you're doing with planning and estimating. Accurately estimating the cost and duration of project tasks can be challenging, and the more you do it, the better you'll get if you spend time looking back at the original plan (e.g., if you thought that the assessment would take three weeks and cost $5,000, and it took seven weeks and cost $9,000, you need to understand why). There are essentially two things to look for: did things go wrong that you should have (or could have) anticipated (i.e., did you just miss something), or did things go wrong that you could not have anticipated. Be extremely honest in your assessment (it's not about blame, it's about understanding how to improve), and look for ways to enhance your overall project planning skills with the team. The better everyone becomes at project planning, especially with respect to identifying key tasks, creating a reasonable and achievable schedule, and developing a realistic budget, the better your project results will be.

Business Intelligence…

Compliance, Reporting and Security

The maze of compliance and reporting issues facing IT security projects can sometimes be daunting. More important, a company may be compliant and not secure or secure and not compliant. The problem is that many of these regulations are either still evolving or they are unclear because they were crafted by people who understood the intent but not the implementation of these measures. That leaves you, the IT security project manager, in the cross-fire. As you evaluate what documentation and compliance reports must be generated throughout the lifecycle of your project, keep in mind that you will have to find a balance. It will do you no good to claim you were fully compliant after a multi-million dollar security breach, nor will it do you any good to claim you had National Security Agency-grade security after a failed compliance audit. Make sure you discuss these challenges with your manager and with the project sponsor, so you don't end up being "thrown under the bus" if things get difficult later. Throughout this book, we've advocated documenting everything thoroughly, clearly, and accurately while being cognizant that these may become legal documents down the road. If you can present a compelling argument for the decisions you make, you may manage to successfully walk that fine line between security and compliance.

Ultimately, compliance is a business issue that must come from the top down in the organization. Much of the regulatory and compliance requirements had their genesis in corporate malfeasance. However unfortunate it is, the primary responsibility for taking "reasonable action" falls on the IT department, because it is the easiest, most clearly defined target. Whenever possible, bring this further into the organization and continue to educate executives and users that compliance is an organizational issue, not just an IT issue.

Summary

Closing out an IT security project includes many of the same tasks as closing out any other IT project. There are, however, a few notable differences. When evaluating security project plan completion, you need to be sure that you have completed all of the tasks in the project or you may subject your network to unexpected security risks. In a typical project, the ramifications of such an oversight are often not as serious as in a security project, so taking extra care to ensure the project is complete before closing it out, is always wise.

During the course of the project, you had issues, change requests, and error logs in which you tracked outstanding items. These should be reviewed and each item in the list should be properly dispatched. Leaving items open is messy and leaves your project exposed to risk. If an item cannot be properly closed, it should be transferred to some other mechanism or tracking system so the project can be closed and so the issue can still be addressed.

Another part of closing out the project is preparing for the implementation, deployment, and/or operational transfer. This is a very important part of the project, because it not only impacts the users' (and the organization's) perception of project success, it also helps ensure that the security measures you've worked so hard to develop are successfully implemented and maintained.

Project close-out is a good time to capture and summarize lessons learned, and to craft best practices based on those lessons. Though this information should be captured in task details throughout the project lifecycle and shared regularly during the security project plan, you should debrief with the IT project team at the end of the project to look at the bigger picture lessons learned and to develop plans for incorporating lessons learned into a future security project plan. Organizations that don't learn often fail. Knowing how to incorporate lessons learned into your processes and procedures will help you make continuous improvements to help your company remain highly competitive in the global marketplace.

Defining and developing project documentation should be part of your security project planning process and at project close-out, these documents should be gathered, summarized (if needed), and archived. Be aware that project documentation may end up in a courtroom some day, if a security breach occurs and litigation follows. While that's a scary thought for many IT professionals, you can (and should) seek legal counsel as to how and when to dispose of or archive project documentation for any security project. That said, normal project procedures included reviewing various project documents and closing or transferring issues. There may be additional documentation required for compliance-based reporting, and those should also be included in your project planning process. At the end of the project, you should have the required documentation for compliance reporting rather than having to step back through the project to define and develop that documentation.

Solutions Fast Track

Evaluating Project Completion

- ☑ Project completion typically occurs when all task work is completed.
- ☑ In security-related projects, ensuring all tasks are 100 percent complete is important to network security. Status reviews and task documentation can help ensure planned work is actually complete.
- ☑ If you've come to the end of your schedule or budget and you haven't yet completed your security project plan, you have a serious security risk that must be resolved.

Closing Issues Log, Change Requests, and Error Reports

- ☑ Closing out issues logs involves reviewing all open issues and determining the appropriate disposition. If an issue is open that needs to be resolved, you cannot close out the project.

- ☑ If an issue needs to be resolved outside the scope of the security project plan, be sure there is an appropriate transfer mechanism available so the issue remains visible and on someone's "to do" list.
- ☑ Change requests should be evaluated and either incorporated or rejected during the security project plan cycle. If there are open change requests, you may have a problem. As with open issues, a change may be needed outside the scope of your security project plan, and it may need to be transferred to the appropriate forum.
- ☑ Although error reports are likely to be hardware- and software-based and, therefore, resolved within the scope of the project, you should check that all open issues have been satisfactorily resolved and documented.

Preparing for Implementation, Deployment, and Operational Transfer

- ☑ All project documentation should be defined in the project definition phase and consistently collected and reviewed during the project plan phase.
- ☑ During project close out, documentation should be updated and finalized for review or archiving.
- ☑ Project documentation can be construed as legal documents related to the security project plan, and should be treated as such. Consult with legal counsel regarding the appropriate storage or disposition of these documents.
- ☑ Implementation, deployment, or operational transfer are all visible aspects of the security project. They present great opportunities to increase the perceived value and success of the security project through flawless execution.
- ☑ Operational transfer is an important connecting point between the IT security project team and those responsible for maintaining security on a day-to-day basis. Be sure to provide

your operations staff with the tools and knowledge needed to successfully monitor, maintain, and improve security.

Reviewing Lessons Learned

- ☑ The lessons learned should be gathered as part of the tasks details and reviewed on a periodic basis with the team.
- ☑ A project close-out debriefing on the lessons learned and the best practices can help team members incorporate the findings and support organizational learning.
- ☑ Improving your project results through reviewing and incorporating lessons learned helps keep your company competitive in the worldwide market.

Documentation and Compliance Reports

- Documentation needed for the project should be defined and developed during the project planning stage.
- Documentation includes project status reports, original project plan, schedule, and budget; revised project plan, schedule, and budget; the actual data vs. the planned data analysis and more.
- Compliance documentation should be defined in the project tasks and task details, so that at the end of the project you will have all of the data and documentation needed for compliance audits or reviews (to the degree possible).
- Compliance documentation will vary depending on the laws and regulations your firm must comply with. Keep in mind that all project documentation related to a security project could become legal documents in the future; therefore, handle it accordingly.