Chapter 1

IT Security Project Management Building Blocks

Solutions in this chapter:

- Corporate Security Project Plan Components
- The True Cost of IT Security
- IT Security Project Success Factors
- Project Constraints
- Corporate Strategy and IT Security
- How Corporate Culture and Policies Impact IT Security

☑ Summary

☑ Solutions Fast Track

Introduction

Let's start by stating two assumptions we're making in this book. First, we're assuming you have a solid understanding of IT project management. If not, we have provided you with a free download of the book *How to Cheat at IT Project Management*_(visit www.syngress.com/solutions to register this book and download the PDF) so you can fill in any gaps you may have. Second, we'll assume that you have a fairly good understanding of network security. This book is not intended to teach you basic IT project management nor is it intended to teach you how to implement specific network security solutions for your particular situation. What this book *will* do is provide an operational framework for you to use in designing your own IT security project plan.

Now that we've gotten those details out of the way, let's talk about network security. It's a massive subject and an enormous undertaking for any network administrator out there in the real world right now. By creating a project plan for addressing network security, you can approach this sometimes onerous task with a well thought-out plan. By creating a comprehensive plan for network security, you can be confident your network is as secure as humanly possible. There is no magic bullet and network security is a never-ending task, but using a consistent methodology will reduce your errors and omissions. In network security, it's often what you overlook that intruders exploit.

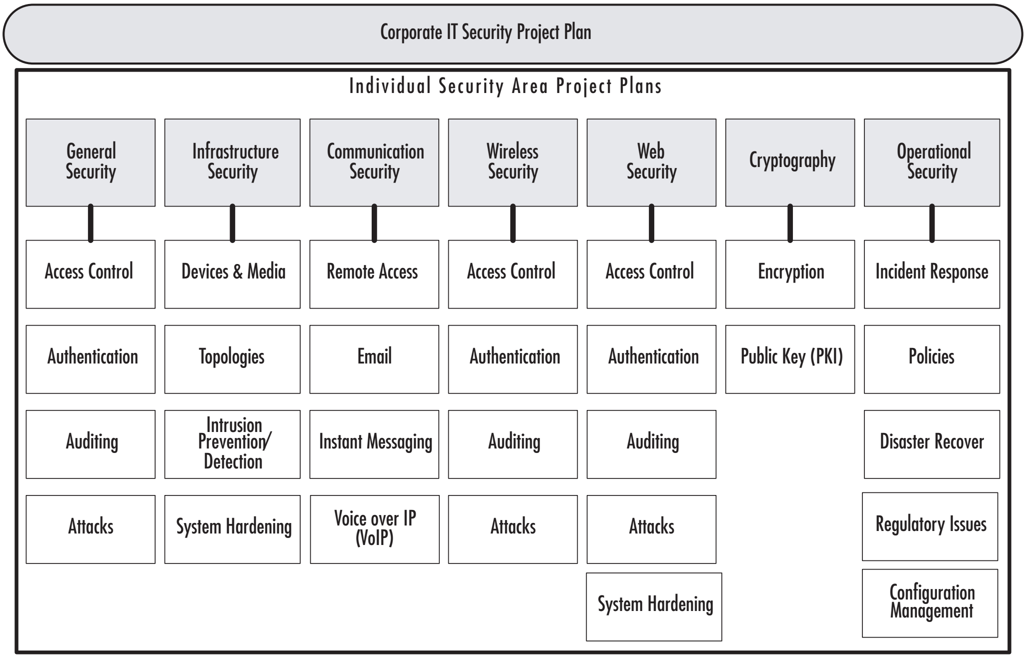
In this chapter, we're going to look at project management from a security planning perspective. We're not going to specifically cover IT project management, but we will use that framework to develop our IT security project plan. This will help reinforce your IT project management skills while providing you with a roadmap for implementing IT security in your organization.

Corporate Security Project Plan Components

Before discussing the specifics of IT security project planning, let's set the stage. Every company has a wide variety of diverse network components that have an effect on security (e.g., users, firewalls, and network topologies). As such, every company usually ends up with one overarching corporate security project plan, and many individual security project plans, each covering a specific area (see Figure 1.1). In formal project management language, the corporate security project plan is considered a "program," which by definition is a related set of project plans that are managed across the enterprise to enable optimal use of resources and to reduce project conflict (i.e., time, cost, resources). To keep it simple, we refer to the "corporate IT security project plan" as the "master plan" and to the sub-level plans as "individual focus areas" or "individual security area project plans." The larger the project, the more difficult it is to manage successfully; therefore, you are more likely to be successful if your corporate security is broken down into small project areas. We'll refer back to this model throughout the book as we explore how to create successful IT security project plans.

One important note at this juncture is that the topic areas included in Figure 1.1 may not be the topic areas you need for your corporate security project plan. You may not need all of these or there may be one or more additional security areas you need to include. The areas listed in Figure 1.1 are commonly used in many organizations but this is not considered an exhaustive list by any means.

Figure 1.1 Corporate Security Project Plan Components



The True Cost of Security

Let's begin with a brief overview of why we even care about network security. If our networks and data didn't need to be secured, we could just leave the gates open and allow anyone in. The reality is obviously far from that. Data needs to be secured because it provides your company with a competitive edge or because it's confidential personal information such as credit card data or social security numbers. There are thousands of reasons why networks and data need to be secured and the unfortunate truth is that there is always someone out there looking for a new way in. That said, it's also true that the majority of security breaches are internal. Whether permissions are incorrectly set allowing a user to access an important file or whether a sophisticated user manages to get a hold of his boss's password in order to look at pay rates or performance reviews; malicious or inadvertent security breaches are most often an inside job.

According to the FBI, nearly 80 percent of security violations are caused by authorized users with legitimate access (i.e., "insiders"). Security threats include disgruntled employees, unsuspecting users, and outside contractors with insider access. U.S. companies spend over $6 billion annually on computer security hardware and software, but the best firewalls and security tools cannot prevent internal security breaches caused by internal issues (e.g., poor end-user security practices, inadvertent mistakes, lax attitudes, employee exploitation of security holes and intentional attacks or hacks).

How much is security worth? Network administrators are constantly under pressure to reduce costs and expand services. A recent study shows that as a percentage of revenues, IT budgets have gone down over the past few years. So, while the actual dollar amount of the corporate budget has risen, the percentage allocated to IT from corporate revenues has dropped (i.e., your company is growing but is not giving you the financial resources you need to do your job). For the sake of argument, let's assume that you have trimmed all the fat from your budget. You are running lean and mean and have no more "give" in your budget. What do you do when push comes to shove? Whatever your answer, it probably directly or indirectly impacts network security (e.g., not having enough IT staff to maintain systems; fewer upgrades to secure operating systems; fewer purchases or upgrades of intrusion detection systems; less time to plan and implement a comprehensive security solution).

So, rather than fall victim to decreasing IT budgets, let's discuss a proactive stance. As discussed in *How to Cheat at IT Project Management* , one of the keys to success in the IT world is understanding the company's business plan. No one is going to hand you a blank check; you have to be savvy. To that end, we look at some quantifiable and verifiable numbers that can be used to develop a strategy for getting your IT security budget approved.

Business Intelligence…

How IT Budgets Are Actually Spent

The February 2006 issue of "CIO Insight Magazine" discusses a research study on IT spending. The conclusions? Many IT professionals agree that their companies do not spend enough on IT (i.e., IT departments are handling an ever-increasing number of projects while IT spending is moving away from hardware and software to staffing and services). The study also surveyed how IT budgets are spent. Interestingly, security software was eighth on the list of technology spending. Disaster recovery and business continuity was first on the list of initiatives. According to Ken Goldstein, an economist with the Conference Board (a business research organization), part of the reason companies are reluctant to spend more on IT is that businesses "haven't gotten full utilization out of what they've already spent, and they need to. They will not necessarily cut back their spending, but what we will get is this cautious, conservative spending." (CIO Insight, February 2006, p. 69.) Making the effort to align IT projects with corporate strategies and to develop and present a business case for key IT projects, continues to be one of the best ways to ensure that your IT department has the tools and resources it needs. Security spending should be a discrete line item in your IT budget. You should prepare the business case for security separately (though in an integrated manner), otherwise it may get lost in the larger IT budget.

Prevention vs. Remediation

One of the best ways to support an increase in IT spending for security, is to clearly delineate the cost of preventing a security breach versus the cost of fixing a security breach. Most corporate executives appreciate a rational approach to the business end of IT, and find a risk analysis and financial overview helpful tools in justifying additional expenditures. A recent study by Computer Economics shows that spending on security is approximately 3 percent of all IT expenditures, which has remained fairly constant for the past three years. Most telling is that security spending has remained constant while other areas of IT spending have fallen over the same period of time. In addition, spending on security has shifted. Many of the efforts made in the past several years to harden networks against attack are paying off in lower remediation efforts.

This is the key take away for IT professionals today in making the business case for security. Security spending in the past has reduced the cost of remediation efforts today. Sometimes it's hard to make the case for something that's absent, but this is an opportunity to tout how successful past efforts have been. If you don't have specific data you can point to, you can generate some realistic estimates. Determine how much you've spent on hardening the network and calculate about how much time that has saved in both IT staff time and in productivity on the network. When the network is attacked, you have three expenses: the IT staff time, the productivity of people trying to use the network and the often more intangible cost to the company's reputation (which sometimes becomes a legal issue with financial implications). If you're hard pressed to figure out how much your company has saved by not having security breaches, do some research and find industry averages applicable to your industry or company size. To assist in that, we've provided a few numbers, courtesy of research by the Computer Economics group. While this data may be generic, it's a good starting point to help you make the business case for the return on investment for past security spending and why it's a good idea to keep spending that money. Here's another hint: Sit down with your company's financial expert and have a few financial metrics generated based on your findings. If you can show a positive return on investment (ROI) or an internal rate of return (IRR), your company's management will have to sit up and pay attention. Along the way, you'll help secure your reputation as someone who understands the *business* of IT.

The independent research firm, Computer Economics, suggests using the following four steps to create a generic ROI for computer security:

1. Analyze the potential economic impact of a security breach (you may want to delineate the potential impact of several different categories of security issues such as virus, phishing, DoS, etc.).

2. Determine the business exposure (network, Internet connectivity, e-commerce intensity, and so on).
3. Examine and delineate the cost of security.
4. Calculate the ROI of security.

For example, if a virus invades your network, you can track how many IT staff hours were required to remediate the situation, by calculating how long you spent fixing the problem (e.g., 60 minutes × 48 users × an average hourly rate based on overall salary levels in the organization). Sometimes, you can determine how much revenue was lost during that time (e.g., if you had to shut down an e-commerce server for four hours, what were the average hourly sales for that particular day and time?) Can you calculate how many of those customers will not return or will spend less in the future? Probably not, but you know the four-hour outage will have a ripple effect that is larger than the calculated hourly loss. In general, some quantifiable data is better than none, and you can use it to begin tracking and analyzing the true cost of security breaches. Some executives only understand the value of security spending when they understand the actual cost of such a breach to the organization.

Potential Economic Impact

In order to understand the potential economic impact of a security breach, you have to look at the cost of remediation and the short- and long-term impact to the organization. The immediate impact of remediation includes the cost of labor and parts to repair damaged systems, the loss of organizational productivity during the repair phase, and the impact these repairs have on the cash flow and financial transactions of the company. If your company is e-commerce-intensive, this impact will likely be even more significant. The loss of security around credit card data or the destruction of a month's worth of e-commerce transaction data clearly has an economic impact beyond the cost of repairing the security breach. Look at all areas of your business where the network and the Internet are factors. (A specific plan to assess the risk to your network is discussed later in this book.) At this point, your goal is to look at the cost of security so that you can make a business case to corporate to gain the necessary organizational, political, and financial support you need for your security projects.

The short-term impact of a security breach (e.g., if your e-commerce site experiences a DOS attack) includes the potential loss of sales and the potential loss of contracts and relationships with suppliers, vendors, and key customers. If your organization has suffered a serious and very public security breach, your sales team might have more difficulty closing a big deal. Clearly, the reputation of the organization suffers and, while it might be difficult to quantify, it reduces the company's reputation and associated "goodwill."

The long-term impact of a security breach includes the loss of key customers, the loss of market confidence, and the erosion of share price if the company is publicly held. The public perception of a company in the marketplace is not built overnight, but it can be destroyed overnight by an avoidable security breach. The news is full of recent examples of companies that inappropriately managed data security and ultimately paid the price. It is hard to recover from that kind of major security lapse, both in the real terms of remediation and in the less tangible terms in the minds of suppliers, customers, shareholders, and the community.

The bottom line is: the more devices attached to your network and the more reliant your company is on the Internet for doing business, the more a security breach will cost. The Computer Economics group estimates that if you are highly reliant on the network and the Internet for your business activities and you have 100 attached devices, the cost of a security breach is approximately $250,000. If you have 250 devices, the cost is approximately $500,000. These costs include cleaning infected systems, recovery from hacks and intrusions, a loss of revenue, and a loss of employee productivity. As you can see, it becomes much easier to justify security-related spending when you clearly delineate the cost of not doing so.

Business Intelligence…

The Real Cost of Remediation

A quick scan of the headlines will tell you that security breaches are on the rise. It takes time and effort to stay one step ahead of hackers. However, a recent report reveals that many companies would rather spend money cleaning up the aftermath of an attack on their network security, than deal with it proactively. Security spending is still seen by some as a giant black hole where money goes in and nothing comes out. However, a glance at the headlines shows that companies that experience massive public security breaches end up in trouble with their customers, their employees, their shareholders, and often the government.

A well-publicized incident in June 2005, involved a serious security breach by CardSystems, a credit card processing company. The company was holding on to credit card data it was not supposed to have in order to "analyze" it. However, the data was not properly secured and 40 million credit card holders' personal data was compromised. Credit card companies had to re-issue millions of credit cards. (MasterCard alone had to re-issue 13.9 million cards.) CardSystems was sold to another company in what appeared to be a "fire sale" in September 2005. After reviewing the incident, the Federal Trade Commission determined there were clear security problems and required the company to have an independent security audit every other year for the next 20 years. This is a classic example of a security breach that could have been avoided. It started on the inside from apparently "benign" behavior (i.e., no one initially attempted to hack the data). The data was stolen because internal procedures violated two areas: their agreement with credit card companies on how they would handle customer data, and their decision not to follow appropriate protocols for monitoring and managing data to ensure its security. (For additional information, go to *www.consumeraffairs.com/news04/2006/02/ftc_cardsystems.html*.)

A Vermont college system employee on vacation in Canada, had her laptop stolen from a locked car. The laptop contained personal and financial data for over 20,000 Vermont college system employees and students. The data was not encrypted. Details about the theft were not

Continued

disclosed for three weeks, even though the data at risk included people's social security numbers, birth dates, bank account numbers, and payroll information. A second security breach involved a hacker using an IT staff person's e-mail address to send a system-wide message regarding the stolen laptop. (For additional information, go to *http://www.burlington-freepress.com/apps/pbcs.dll/article?AID=/20060409/NEWS01/604090316/1009/NEWS05.*

A security breach in Spokane, Washington left hundreds of bank and credit union debit card customers in a tight spot when they were informed their debit cards had been compromised. New cards and PIN numbers were issued. The breach cost banks, credit unions, and customers thousands of hours for canceling and re-issuing debit cards. The cost to banks, credit unions, and customers ran into the hundreds of thousands of dollars. (For additional information, go to *http://www.kxly.com/news/index.php?sect_rank=1&story_id=1253*.)

Security spending is time and money well spent. Your job as the network administrator is to make the business case for security spending. One way is to align security goals with business goals. When you tie security to business objectives, senior executives are more likely to understand, value, support, and fund security initiatives.

Business Exposure

This section discusses the relative exposure of your business, which will help you present your business case for security-related spending, and help you gain critical support for your IT security project. Some business exposure can be assessed by looking at the following categories and determining what percentage of your business they comprise:

1. **E-commerce Retail Sales** If your company sells product via the Internet, there are numerous security issues that must be addressed. From Web site security to transaction security, and from credit card processing to identifiable user information, your company has a legal and ethical obligation to maintain a certain level of security.
2. **Business-to-business (B2B) Transactions** Some companies only deal with other businesses (i.e., not the general public). These B2B transactions are vulnerable to outside and inside attacks. Disruption of this revenue stream can be devastating, because it can damage a

company's cash flow and its relationship with key business partners (i.e., eroding trust and confidence reduces the value of the business transaction).

3. **Internet Connectivity and Reliance** Some companies rely heavily on the Internet. If your company uses the Internet to connect with customers, vendors, regulatory authorities, employees, or shareholders, you must assess the risk of loss or disruption in each of those categories. The more you rely on the Internet as a business tool, the greater your need for tight security and additional security funds.
4. **Dispersed Workforce.** If your company's employees work from home, work on the road, connect from airports, coffee shops or vendor's locations, your network security needs to take this workforce model into account. The risks to the network obviously increase when users are roaming around out in the wild unsecured world of coffee shop (or hotel) wireless networks and your network security plan has to account for these types of arrangements.
5. **Electronic Data Interchange with Businesses and Consumers** You risk a security breach whenever you exchange data directly across the Internet. There are numerous technologies that will secure those exchanges.
6. **Data Sensitivity** Legislation regarding the privacy of medical history and other personal data (e.g., social security numbers, credit card numbers, household income, credit scores, and so on) has expanded. Any company dealing with confidential personal information must have strong security processes in place to ensure that the data is handled properly at all stages (i.e., from collection to storage, retrieval, and analysis). Disruptions in this area can result in serious financial and legal consequences.

Cost of Security

The amount of money spent on security should match the risks associated with a potential breach of security (e.g., a financial firm has a higher risk profile than a paper supply company). However, both companies must assess their risk and decide on a reasonable level of protection. You can spend a lot of money on security, but at some point your ROI diminishes because you are outspending your risk.

When planning for the cost of security, evaluate the following:

- Company size
- Nature of company business
- Government regulations
- Reliance on e-commerce, Internet, and network connectivity
- Nature of business transactions
- Business structure (centralized, multiple locations, mobile workforce, and so on)
- The tangible and intangible value of the information and company data
- The potential impact of a security breach on the company's reputation and bottom line

One point that can be easy to miss in all of this is that your security really should be calibrated to the value of your company's data. To use an analogy, there's no point on putting a $5,000 alarm system on a 1979 Chevrolet Cavalier that has a rusted out frame and 150,000 miles on it. It's probably pretty low on the list of cars that get stolen (no offense intended toward anyone who owns such a vehicle, but chances are you don't worry about it getting hot wired in your driveway). On the other hand, if you own a $250,000 custom sports car, a $5,000 alarm system might not be enough. You might also add a low-jack system that disables the engine when the car is reported stolen and you might also install a GPS tracking device so you can locate the vehicle if it is stolen. The point is that your security measures need to really take into account the value of the data and the potential impact if that data (or network services) are disrupted. However, since you will have defend your budget, you also need to make sure your security solution is commensurate with the value of the data and network services and the relative cost of business disruption.

ROI of Security

Once you have delineated the cost of security threats and security spending, you can calculate a ROI or do a break-even analysis. The Computer Economics group determined that for a company with high exposure to risk factors (e.g., e-commerce companies), the break-even point for security per device is approximately $375 for a company with 100 devices. The per-device cost is approximately $400 for a company with 500 devices, or about $250,000. For the following example, we use a 100-device network. The cost for security hardware, software, implementation, management, and personnel is estimated to be $196,000 for a high risk company. The cost of a single security breach is estimated at $233,000. While this appears to be a $37,000 savings, it may not adequately address the loss of productivity, opportunity costs (e.g., What else could we have done with our time if we were not remediating a security breach?) and the cost of the black mark on your business's reputation. The numbers show that the cost of avoiding a problem is less than the cost of fixing a problem. Put some numbers together for your organization that show the net positive result of problem avoidance. (For more information on the economics of computer security, go to *www.computereconomics.com*.)

Business Intelligence…

The Ultimate Cost of Security

A recently released survey by CompTIA sheds light on the cost of security. (See The Channel Insider, "Poll: IT Security Training Not a Priority" by Pedro Periera at *http://www.thechannelinsider.com/article2/0,1895,1934496,00.asp*).

According to CompTIA Chief Operating Officer (COO) Brian McCarthy, employers do not invest in enough training; fewer than 25 percent of employees receive any type of security training. While the investment in security hardware and software has increased in recent years, the investment in training has not kept pace, which is alarming when you consider

Continued

that 80 percent of all security breaches are caused internally, many due to simple human error. Much of that error can be directly attributed to a lack of security training. Companies have a false sense of security when they look at the capital investments they make in hardware and software solutions, but without adequate training on the proper configuration, use, and maintenance of the security solutions, those capital investments are wasted. The survey also found that, on average, IT departments spend 2 percent of their time and 5 percent of their budgets on security. That is pretty low when you consider that the average security breach typically costs a company approximately 1.5× what they spend on security solutions.

Now for the cold hard truth. According to the Gartner Group, 50 percent of all businesses that suffer a data loss due to an attack or system failure, go out of business within three years of the attack if they fail to restore the lost data within 24 hours.

Project Success Factors

In ITPM, we discussed the factors that contribute to project success. These factors bear repeating because they are significant when it comes to IT security. As we step through these success factors, we will look at them with an eye toward IT security. As you are reading, you may find there are additional nuances to these elements that are unique to your company or organization. If so, make a note for future reference. Understanding project success factors will make your job easier as you plan and implement your project.

Success Factor 1: Executive Support

The number one success factor of any project is executive support. If company executives do not understand or care about a project, they will not allocate the time, money, or resources needed to make it successful. Most corporate executives are aware of the need for IT security; however, if management is still not taking IT security seriously enough, you will have to embark on an education campaign to help them understand the importance of sound IT security planning. Like an insurance policy, the cost of having a sound IT security plan it is almost always less than the cost of not having one.

IT security is not inexpensive. The cost of labor to assess, plan, implement, manage, monitor, and respond is expensive. Add to that the layers of hardware and software components needed to keep IT secure, and you start seeing IT dollars disappear. Without executive support for IT security planning and implementation, it will be hard to get IT security budgets approved.

Business Intelligence…

Executive Support 101

In most companies, the easiest way to gain executive support for IT security spending is to make the business case for the expenditures. Tying IT security in with the corporate strategy, mission, values, and goals can help executives understand and approve needed expenditures. A little aversive therapy also goes a long way (e.g., get examples of companies, ideally in your industry or segment, that have had security breaches. Highlight not only what the ultimate cost of remediation was, but also how embarrassing it was to the company. It only takes one or two good examples to help executives understand that they do not want to pay the clean up cost when the prevention cost is lower.

Without executive support, IT security initiatives will ultimately fail because the organization will allocate time and resources to other projects. There are numerous competing demands and priorities in every company. If your executive team does not understand or value security initiatives, you will have an uphill battle. Organizations need to develop a corporate culture that supports security from the ground up; however, this can only be created when there is support and active involvement at the top. Most security breaches happen inside the organization; therefore, developing a security culture is critical to maintaining IT security. Do your homework, make the business case, and give your corporate leaders the tools they need to make informed decisions that support IT security.

Success Factor 2: User Involvement

Most security breaches occur from inside an organization. Some breaches are intentional and some are completely innocent, but the net result is the same—security is compromised and the company is put at risk. Users often view security differently than IT employees, which is why there is poor communication between the two groups. The user's view is, "I need to access everything at the same time." The IT perspective is, "You need as little access to as few resources as possible." Neither perspective in the extreme is useful; there has to be a balance between the two. By involving key users in your security planning process, you will have the "real world" perspective at the table. Hearing user's objections to security measures will allow you to modify them accordingly.

A good example of that balance is *password policies*. If you require a 10-digit minimum length password that must be changed every two days, there is a high likelihood that users will write the passwords down at their desks so that they do not forget them. This type of security circumvention occurs because the users were not consulted when the security policies were created. In most cases, however, if you can find a balance between the user's needs and the security needs of the organization, you are more likely to see higher user compliance. When you involve key users in the process, you avoid having them circumvent policies that are too stringent and you avoid having to revise your policy after it fails.

Success Factor 3: Experienced Project Manager

In the case of IT security, it is critical that the project manager have experience successfully managing projects, since any errors or omissions in a security plan can have serious consequences. A project manager using a proven, consistent project management methodology is more likely to generate a solid IT security project plan than one who has no consistent method for approaching an IT project. If you are the project manager for your company's IT security project and you are not an experienced project manager, look within your organization or your professional associations for a mentor to assist you in developing your plan. Depending on the size and scope of your project, you may choose to hire an experienced consultant to work side-by-side with, so that you can avoid some of the common pitfalls inexperienced IT project managers face.

Success Factor 4: Clearly Defined Project Objectives

Successful projects begin with clear definitions of what the project entails. More often than not, an unsuccessful project lacks a clear, concise definition. You typically begin by identifying the problem and then identifying the desired outcome (or mission) of the project. By identifying the problem that is driving the need for this project along with the desired (or required) outcome, you will identify the gap between what is and what needs to be. From there, you are in a better position to clearly define project objectives. The key is that the objectives be clear and unambiguous. You should ideally develop three to five major objectives for your security project. (Defining project objectives is discussed in more detail later in this book.)

Business Intelligence…

The Power of Clarity

In my consulting work, I often see people launch into projects without a clear sense of direction, whether the project is self-initiated or handed to them by a client, boss, or co-worker. Stepping back and asking what outcome you are trying to achieve and what the major objectives are will bring clarity to your project. When defining your IT security project, you want to define three to five major objectives that will drive IT security for your firm. Be very clear about what you are trying to achieve and you will have a much better chance of achieving it.

Success Factor 5: Clearly Defined (and Smaller) Scope

Studies consistently show that projects that are clearly defined and smaller in scope are more successful than those that are not. Whenever you start a project, you should always begin with the project objectives. The planning process should develop your top three to five high-level objectives into smaller tasks that eventually define your entire project from start to finish. When a project is clearly defined, it is easier to see if it is missing any elements or if it is hitting the mark.

Another success element is having a smaller scope. A scope is defined as the total amount of work to be accomplished for a project. The smaller the scope, the more likely that the project will be successful. The bigger the project, the more elements there are, resulting in the likelihood that one or more of them will be overlooked. In recognition of this important success factor, this book approaches IT security as a series of project plans, not one big plan. The overarching IT security plan includes sub-plans for each IT security area. To some extent, each of those sub-plans can be managed as separate plans. By defining sub-plans for each individual security area, you can accomplish two important goals: 1) you can assign the right people to the project based on their areas of expertise, and 2) you can focus intently on that aspect of security so that all of the key elements are addressed.

Success Factor 6: Shorter Schedules, Multiple Milestones

With a smaller scope come shorter schedules. Again, this is fairly intuitive. It is hard to plan far into the future because so many intervening factors can arise over the course of 6, 9, or 12 months. Keeping shorter schedules means reducing project scope. One of the ways to do this with IT security is to divide your security planning into segments (as we have done for this book.)

Another interesting statistic is that projects with multiple milestones are far more successful than those with few milestones. By definition, a milestone is a marker in a project plan that indicates a significant event. It can be a checkpoint to ensure everything is on track, or it can be a checkpoint that indicates that some external event must be completed before the project can proceed. It is like directions to a location you have never been to before. If you read them once before heading out, you are likely to get lost along the way. On the other hand, if you read the directions along the way, you are more likely to turn left when you should turn left and right when you should turn right. Multiple milestones help you navigate time and schedules more effectively.

Success Factor 7: Clearly Defined Project Management Process

If you use a consistent process for defining, implementing, and managing projects, you are more likely to produce successful projects. Again, it is a process that should be implemented to help ensure that you include key elements in the right order at the right time. If you do not have a consistent project management process, you should develop one. (ITPM provides a methodology that you can use to cover the key elements of project planning.)

Success Factor 8: Standard Infrastructure

When developing your IT security project plan, look for opportunities to use standardized components, from software and hardware infrastructure elements to templates and off-the-shelf solutions. Carefully analyze the cost of purchasing infrastructure versus creating your own. Small- and medium-sized companies often fall victim to the "it costs too much" mentality when looking at off-the-shelf solutions to incorporate into their products or projects. However, if you add in the cost of errors, omissions, re-work, and cost and schedule overruns, you will probably find that purchasing these components or elements is a better business decision, even if it costs more than you expected. In addition, re-using standard templates and sections of IT project plans for your IT security plan enables you to avoid reinventing the wheel and will yield more consistent results over time.

Project Constraints

This section covers project constraints as they pertain to IT security project planning. If this is not a concept you are familiar with, refer to Chapter 1 in ITPM for a more detailed explanation.

Every project has four constraints: scope, time, cost, and quality. The relationship between these elements is described by different people in different ways, but the essential understanding is that there is a relationship between these elements. The total amount of work that can be accomplished (scope) is determined by how much time you have, how much you are willing to spend, and what level of quality is required. Conversely, the amount of time you need to complete a project is related to what you are willing to spend, what level of quality is required, and how much work you need to accomplish. The relationship is often shown in this manner:

Scope = Time x Cost x Quality

Let's look at the reverse of this. If you define a project and your division manager says that it is fine except you have to reduce the cost by 30 percent, you are forced to make some hard decisions. You can reduce the scope of work to reduce the cost, or you can reduce the quality to reduce the cost. If you change one of the constraints you also have to change another one. Changing one constraint without revisiting the others sets the project up for failure.

The scope of an IT security project can be defined by the IT security master plan or sub-plans. Reducing the scope allows you to reduce the time and cost of the project while still delivering high quality. Ideally, you should create an IT security project plan overview and then create separate sub-plans, which will allow you to manage the scope, time, cost, and quality more effectively.

In addition to understanding the interaction of the four constraints in a project, it is also important to understand how to prioritize those constraints. In every project, one constraint is typically "etched in stone" (e.g., the executive team tells you that your project cannot exceed $100,000 or that it must be completed within 6 months maximum). When you have this type of constraint, you have to make the other constraints more flexible. For example, suppose that in 12 months your company is going public through an Initial Public Offering (IPO). As part of the rigorous process, your company wants to make sure its network security is firmly in place at least 6 months prior to the IPO. Therefore, you are given 6 months to put your network security plan in place. Depending on a number of factors (e.g., how large your network is, what security is already in place), you may determine that 6 months is manageable only if you hire outside security consultants for assistance. That means that because time is the top priority and least flexible constraint in this project, you have to be more flexible with the other constraints. In this case, the cost will probably increase to accommodate the constraint. If the company executives are inflexible on all four constraints, the project will probably fail.

There is a saying in project management that states, "Things are more likely to go wrong than they are to go right." If the four project constraints are etched in stone, you have little chance for success. Increase your odds by negotiating with the executive team for one or more flexible constraints. That doesn't mean they open the checkbook and let you spend without limit. It does mean that they will need to understand that with a hard deadline that is fairly aggressive, they will have to give on the cost or the scope. If they refuse, the result will be what typically happens in many organizations. The team agrees to unrealistic targets because it really has no choice and then it fails to meet those targets because they were unrealistic. The plan changes in the middle of the project because something has to give way. Saying that it's not allowed to happen doesn't prevent it from happening. Negotiate up front for realistic parameters and priorities so that everyone benefits.

Corporate Strategy and IT Security

What does corporate strategy have to do with IT security? Suppose that over the next three to five years, your firm's strategy is to gain market share through the strategic acquisition of targeted companies in select geographic regions of the U.S. As network administrator, you must ensure that your corporate IT assets are protected today, while also making sure that new locations can be incorporated in the future. Each company acquired has its own network infrastructure, security policies, and tools for managing security. How you seamlessly integrate these acquisitions into your company and still keep all IT assets secure should be part of your IT security project plan.

Let's look at another example. Your company manufactures several products that are sold by mass merchandisers around the world. To remain competitive against the influx of low-cost alternatives to your products, your company decides it needs to improve its supply chain and distribution channel management. Part of that initiative involves providing suppliers and customers with real-time access to production and shipping data. This initiative would impact IT security by opening your network to vendors on one side and customers on the other, thereby exposing your network to a host of new, potential security problems.

It is critical that you are intimately aware of your company's short- and long-term strategies in order to effectively plan, implement, and manage IT security. If you do not understand how IT resources are used today and how they will be used tomorrow, you will not be able to create and manage a successful IT security project. Reworking a plan is expensive and results in a lot of wasted time and effort. Rework can be reduced by looking ahead at corporate strategies, at where your company is headed. If you align your IT security project with corporate goals at the project outset, you avoid some rework. That said, the business world is a dynamic environment and it is guaranteed that plans will change. If you start out closely aligned, you may be able to make minor modifications rather than wholesale changes to your security plan.

How Corporate Culture and Policies Impact IT Security

In addition to clearly understanding and aligning with your company's strategies, you also need to understand its culture and policies. Every company has a unique culture. Some companies have a very lax "we are all friends here" culture, where rules are few and seldom enforced. Others have very formal "buttoned down" cultures, where managers are addressed as "Mr. Brown" or "Ms. Black," and where rules are many and conscientiously enforced and obeyed. If your IT security policy does not address the reality of your corporate culture, it will not be effective. If you establish 52 rules of network security in a company where things run rather fast and loose, 51 of those rules will be disregarded whenever possible.You cannot single-handedly change your corporate culture, but you can influence it greatly when it comes to IT security. If you educate executives and users about the importance of IT security and how it affects them, you are more likely to gain their support and compliance.The reverse is also true. If you work in an environment where rules and regulations sometimes overwhelm even the simplest business process, you may need to make a case for having a more relaxed environment. Again, the complex password scenario is the one that consistently comes to mind. If you require passwords that look like *x%v93P!2m5>6*, users are going to write them down even if it is against the rules.

Company policies also come into play when creating an IT security plan. Does your company require a background check on employees who handle money, manage confidential personnel files, or who have full administrative rights on the network? Does your company have policies in place that address current regulatory requirements such as Health Insurance Portability and Accountability Act (HIPAA) or Sarbanes-Oxley (SOX)? If so, your IT security plans should also address these policies. Reviewing corporate policies will help you align your IT security with the requirements and realities of your company. Make sure you include legal, financial, and human resources representatives on the IT security project team, which will help ensure policies related to network security are properly addressed.

And finally, if you include users (Success Factor #2) in your security planning project, you are much more likely to strike a balance between the need for tight network security and the need for users to easily access the necessary resources. If you neglect to bring users into the mix until you are ready to implement the security solution, you will probably find that users are more resistant because you are simply "laying down the law." A collaborative approach, while taking more time in the planning stages, generates a better result and reduces problems in the implementation stage. The cost of making changes to a project in the planning stage is significantly less than making changes in the implementation stage; therefore, including users early in the process will save you time and money in the long run.

Summary

In this chapter, we looked at the underlying rationale for why it is important to have a sound IT security project plan prior to implementing IT security solutions. Every IT initiative must be funded, and IT security is no exception. While most executives understand the risks in today's connected world, many are still reluctant to authorize IT budget increases or to wholeheartedly support security initiatives.Your job is to make a business case for IT security spending through developing a sound analysis of the economic impact of a potential security breach, the risk profile of your company, and the cost of prevention. With this data, you can develop an approximate ROI calculation that will make sense to any corporate executive.

We also looked at the success factors of security projects. Executive support is key for two primary reasons. First, they have to authorize the financial expenditures. Second, without their support, the project is likely to fall off the list of key initiatives or corporate priorities, which means you will eventually be scrambling to find the time and resources needed to complete the project. User involvement is the second success factor. Involving users early in the planning process may seem like a major inconvenience; however, their involvement will help ensure that the implementation phase of your project goes more smoothly. Ultimately, user involvement will help you create a better project plan. Other success factors include having an experienced project manager who can ensure that the project scope, time, and processes are well-managed.

Each project has four constraints, which must be balanced and prioritized. It is important to understand that if you increase the scope, you also have to change one or more of the project's other constraints. Conversely, if you reduce the budget, you also have to change one or more of the project's constraints. It is also helpful to understand the priorities of these constraints. If there is a hard budget or a hard deadline, the other project constraints must be flexible to accommodate the inevitable problems and changes that occur during the implementation phase of the project.

Mandating all four constraints results in project failure on one or more fronts.

Another critical element to the success of your IT security project is understanding where your company is headed to in the future. If you craft an IT security plan that fails to account for possible future activities of your company, you will have to continually change your plan or you will have gaping security holes. Rather than continually reworking your plan, try to determine where your company is headed in the next three years and then plan accordingly. While this will not eliminate change to your IT security plan, it should help reduce it to a minimum.

As you develop your IT security policy, look at your company's culture. While you may have to implement new rules and regulations where none exist, you should try to align your security planning with the corporate culture to the greatest degree possible. When you do, you increase the likelihood that users will comply with IT security requirements. You may also need to work collaboratively with various stakeholders within the organization (e.g., Human Resources, Finance, Legal and so on) to ensure that the IT security policies match the corporate culture and the existing company rules, regulations, policies, and legal requirements. Creating an IT security policy in a vacuum will yield less than optimal results, if not outright failure.

Solutions Fast Track

The True Cost of IT Security

☑ According to FBI statistics, 80 percent of corporate security breaches occur from within the organization.

☑ Despite the initial cost of security hardware, software, and planning, prevention is usually less expensive than remediation.

☑ Many firms fail to take into account the "soft" costs of security breaches, including opportunity costs, cost to the reputation of the firm, and residual costs in the marketplace.

☑ When making a business case for IT security spending, assess the economic impact of a security breach, determine your company's level of risk, determine the cost of prevention and the value of the data, and calculate the ROI.

☑ Many companies fail to provide adequate training; errors account for a majority of security breaches. Training is key to the successful implementation of a security plan.

☑ Fifty percent of all businesses that suffer an attack or data loss go out of business within three years if they fail to recover from the data loss within 24 hours.

IT Security Project Success Factors

☑ Executive support is key to the success of all projects, but even more so to IT projects that require capital expenditures and cultural and political support.

☑ If users are not involved with the decisions regarding security implementation, there is a high likelihood that they will fail to comply or will actively seek ways to circumvent security.

☑ An experienced project manager contributes to IT security project success in many ways. Among them, he or she helps to clearly define project objectives, manage the scope of the project, create meaningful milestones, and develop project processes that foster success.

☑ Whenever possible, standardizing project infrastructure reduces the cost and time of the project. If you can reuse tools, processes, or methods from other projects, or if you can implement standardized tools or equipment, your projects will typically generate better results by reducing the learning curve and ramp-up time (which often leads to errors and omissions).

Project Constraints

- ☑ All projects have four constraints that must be balanced throughout the project. The scope (total amount of work to be done), the cost (budget), the time (schedule), and the quality.
- ☑ If you increase or reduce any element, one or more of the other constraints must change. If you reduce the cost of the project, you must increase the time or reduce the scope or quality of the project.
- ☑ Studies have consistently shown that projects that are shorter in length and smaller in scope tend to be more successful. One useful strategy is dividing your total IT security plan into multiple sub-plans. You can keep an eye on the overall IT security picture through a master IT security plan with multiple sub-plans incorporated.
- ☑ Gain agreement as to project priorities prior to the start of the project. Negotiate for one or more flexible constraints, since mandating all four constraints almost always results in the project failing to meet those parameters.

Corporate Strategy and IT Security

- ☑ While developing your IT security plan, you must take into account your company's strategy.
- ☑ Understanding where your company is headed and how it plans on getting there will enable you to develop an IT security plan that will meet the current and future needs of the organization.
- ☑ Developing an IT security plan that addresses the company's short- and long-term goals is important, but keep in mind that companies have to remain flexible and nimble to survive in today's global economy. Your IT security plans should be equally nimble to address the constant change your firm is experiencing.

How Corporate Culture and Policies Impact IT Security

☑ Companies all have very unique cultures. It would be imprudent to disregard the corporate culture when developing an IT security project plan.

☑ When developing security policies, look at your corporate culture and determine the most effective ways to implement security. Including users and key stakeholders from various parts of the organization in the security planning process, will help ensure that you implement policies consistent with user behavior.