CHAPTER

1

Setting the Stage for Successful Security Planning

Security isn't a product, a feature, or anything that we can simply acquire and then implement, confident that it will work now and forever after. It is a highly complex, organic process, one we must manage heuristically and optimize in an ongoing process. Security is also a way of thinking; it is neither an absolute science nor a purely technical subject. Security planning demands an understanding of the psychology of the hacker, of the key variables influencing information and infrastructure vulnerability, and of the organization's business. Security also requires a framework for weighing these variables, for the purpose of driving security implementation decisions and associated budgets.

This chapter sets the stage for a security planning approach that works. Along the way, we'll identify the challenges, problems, and pitfalls associated with less-than-optimal approaches so that we know how to avoid them. We will address the important topics of security risk (impact) analysis, to give our security plan focus and justification. To that end, the chapter introduces a method for guiding and justifying your security budget and addresses the important topic of successfully "selling" security inside your organization. The chapter closes with a summary of security business process improvement. All of the topics introduced are then expanded on throughout the remainder of the book.

TIP **Refer to the comprehensive glossary of this book whenever you see a term or an acronym you don't understand.**

Not an Absolute Science

Protecting information or defending a computing infrastructure is not an absolute science. Effective security planning requires that we understand the relative value of what we're protecting, the cost of protecting it, and the probability that what we're protecting will be violated in spite of the security measures we put into place. Security planning is also about learning to manage the tradeoff between these things—think of the process as balancing a "security diet."

A balanced security diet incorporates the realization that security is about managing risk in an environment with limitations, *not* about finding a way to prevent loss at any cost and level of inconvenience. As with any diet, attempts to impose overly rigid security measures will paralyze an organization, causing it to adopt, as a knee-jerk reaction, too few security measures. This is tantamount to saying there's no value to locking doors and windows in a house because someone can just break them; therefore, we might as well leave the windows and doors unlocked and instead arm ourselves with a submachine gun. Such an attitude will result in an unbalanced security environment.

As we'll see throughout this book, security is not a single thing. Optimal configuration of a firewall, for example, is not security. Nor is a powerful virus scanner or an intrusion detection system (IDS). Security touches every aspect of an organization, from physical security starting at the front door of its buildings to detailed and tedious details about the way we configure our networks to how we run our infrastructure to the information we provide when we answer our phones. It's far broader even than these examples. In Chapter 2, we'll start the process of defining security in terms of a well-structured security technology model, business model, and a view of the life cycle management of security. In doing so, we'll have the beginnings of a security planning approach that will work for your organization. But before we do that, we need to establish an effective mind-set for security planning.

A Way of Thinking

Security is a way of thinking, and we need to think it through better than our adversaries. Effective security planning is the way we accomplish that. But though most of us instinctively believe planning is a good idea, when it comes to complex and difficult-to-manage problems like security, we sometimes resist. This is understandable for two basic reasons. First, because we are on tight budgets and under difficult time constraints, we look for steps we can skip. Second, security is a difficult problem to solve, and we feel we don't have the time it takes to address it adequately. But, as most of us are learning, time and again, we'll be hacked repeatedly unless we take the time to do security right. Ultimately, we come to accept that security planning is a *requirement*, not an optional exercise.

Avoiding the Pitfalls

Once we accept the value of planning, however, we often open the door to some of the problems associated with it. In general, planning, whether for security purposes or anything else, is frequently practiced ineffectively in large organizations. In addition to those who use planning (whether intentionally or not) to escape real work (and so impede, rather than aid, progress), most of us have seen the planning process taken to extremes by the types of planners characterized here as the *ultra-planner*, the *nonplanner*, and the *shock-advisor*.

The Ultra-Planner

For the ultra-planner, planning is its own end, not the means to a more important end. As you might guess, there are many ultra-planners in the security arena. You know the scenario: While you and your colleagues are focusing on securing your organization's information and data infrastructure against hacker threats, the ultra-planner is talking to you about protecting against the business equivalent of sandstorms and locusts. To the ultra-planner, focus is for small thinkers; your insistence that the scope be narrowed only reinforces what a small thinker you must be.

In fact, a lack of focus is the enemy of security. Security administrators routinely admit that one of the biggest challenges they face is deciding which of the hundreds of known security flaws they should protect against at any given time because they do not have the resources to address all of them. Solving the problem requires knowing what to focus on. But to do that, you need to genuinely understand, starting at least from a technology standpoint, which classifications of problems truly apply to you. To do that, you need to understand the underlying technologies; for example, you need to understand that one way to deal with the 100 risks relating to a particular protocol is simply to disable that protocol altogether, or at least isolate it onto its own Ethernet segment where it can be more carefully controlled and monitored. In this example, not only is there a technology issue (understanding what the protocol is and what it means to disable it), but there's a business issue as well: understanding why anyone might need it within your organization in the first place.

The issue of focus is prevalent throughout the book, as you'll see in examples such as this one; learning from these examples will help you develop your own security plan.

AN EFFECTIVE SECURITY PLANNER

An effective security planner combines a good understanding of technology, the planning process, and business implications. These things are necessary to go beyond believing we're safer to truly being safer.

The Nonplanner

The nonplanner is the cowboy in all of us. We think we can "just do it": shoot from the hip and move on. When we're in this mode (and most of us fall into it at one time or another), we become very busy. We put lots of effort and energy into our work, but we know, in the end, that we weren't nearly as efficient as we could have or should have been.

We are then reminded of the value of planning the right way. That's when we sit back down and consider more carefully how to proceed. This and future chapters will direct you where to go, and you'll discover a planning path that works for you, one that is practical, comprehensible, and implementable.

The Shock-Advisor

In many organizations today, the state-of-the-art security planner plays the role of the shock-advisor. This resident security expert typically finds himself or herself in a temporary position of power, generally as a result of a recent security breach. As a result of the breach, staff, many—or most—of whom were only peripherally concerned with security issues, have received a wake-up call, so they are alarmed and ready to listen.

Going from meeting to meeting, the shock-advisor warns everyone that if they don't pay attention, another breach is bound to happen—and with potentially worse results. "You fools," the advisor's words imply, "do as I say or lose it all." Unfortunately, over time, people simply do not respond to these dire warnings; they tune out, turn off. In short, the shock approach doesn't work more than once or twice. And without a change in tactics, things return to the way they were with little or no difference. The point is, we need to *sell* security, not *force-feed* it.

In conclusion, the hard lesson we must learn about security is that we can't go from one extreme or another. What we need—what we *know* we need—is a balanced approach to security planning. Without balanced planning, we are not nearly as secure as we could and should be.

Identifying Risk

If security is a way of thinking, one aspect of this way of thinking is to operate, to a certain degree, in a state of suspicion, so that you can identify the risks your business faces and distinguish between the real and the imagined. For example, you should understand that hackers are becoming more professional. They are more than young adults who are very good with computers and who satisfy themselves by showing you how vulnerable you are. Increasingly, hackers are paid professionals who intend either to extort money from you or to sell your secrets to the highest bidder. Even if yours is a small, relatively unknown company, your systems may be hijacked and used by hackers attacking others.

For example, one company I know of had spread workstations around its customer conference rooms for the purpose of demonstrating its products. These workstations gave unbridled access to all internal corporate and development systems. Such a setup is not unusual: I find this same scenario in four out of five companies (I recommend that you check yours).

Hackers and others engaged in corporate espionage visited this customer conference center disguised as potential customers; they slipped right past front-door security—that is, they didn't even need to be known by anyone to gain access to the customer conference area. Information and infrastructure security starts with strong building security, yet this is one of the weakest areas of security for most organizations.

BAD HACKER, GOOD HACKER

It's important to note that using the term *hacker* in a negative connotation is a misnomer because initially the term referred not to a "bad guy," but rather to someone who was engrossed in computer technology—a computerphile, if you will. The term is now commonly used to refer to someone attacking your information or infrastructure. Twenty years ago, many people referred to me as a hacker simply because I was proficient with computers. To confuse matters further, some now use *hacker* to refer to a "good security person"; they use *cracker* or other terminology to refer to an unwanted attacker. The meaning of the term *hacker* is, therefore, not standardized. What's somewhat new is the commonplace interpretation of the word to refer to an attacker. In this book, I keep it simple: When I talk about a hacker, unless otherwise stated, I'm talking about an attacker of one kind or another.

The point here is this: Security is much more than identifying the risks presented by your network connections. In addition to attacking you via the Internet, hackers disguised as customers, repair technicians, and contractors look for open cubicles, offices, and, especially, empty conference rooms having LAN connections to the corporate network. They call on the phone and extract private information. Lazy hackers or those not so adept at conning the receptionist often simply sit out in the parking lot with a wireless 802.11b-enabled notebook computer and access many corporate networks behind the firewall, an invasion made possible because corporations are increasingly using wireless networks, many of which offer no security.

These types of intrusion are so prevalent now that if someone doesn't believe it's as easy as I say it is and challenges me to prove it, I can "break in" almost on demand. While unknowing victims feel secure with their firewall investment, these hackers just walk right into the building or use the telephone and get what they're after. As this book will demonstrate over and over, security is not about any one feature. Security is not a firewall.

Profiling Hackers

To be a successful security planner, you will help your organization understand and appreciate what and where the real risks are. As part of this undertaking, you need to familiarize yourself with the various types of hackers and their range of motivations. Those who attack your information or infrastructure fall into the following primary categories: the attention seeker, the malicious, the curious, the thief, and the unintentional hacker. All present considerable danger. Let's profile them one by one.

The Attention Seeker

Attention seekers are the most common variant of attacker. They attack systems for the pleasure of showing off their hacking skills. They enjoy being noticed and particularly relish the press exposure associated with revealing a flaw in a major organization's system.

Often the best way to deal with such attackers is to give them the attention they seek; that is, give them your full attention, as opposed to giving an attacker the opportunity to make the attack widely known—in short, a PR nightmare. If possible, keep the attack quiet, at least until you can notify the affected parties in an effective way and get people working to remove the security vulnerability. In parallel with all of this, you should turn your attention to the attacker: Make him or her feel important. Learn everything you can from the attacker about your vulnerabilities. Often these people just want to be heard—and well they should be, for they have valuable information to share.

Though not everyone would agree with me, I also consider it reasonable to compensate these individuals with gifts or payment. Those who consider this "extortion" fail to factor in the motivations of this type of hacker. They aren't directly asking you for money or gifts; it's your attention that motivates them. Typically, they are not trying to hurt you. Furthermore, taking an openly provocative posture with a hacker is not in anyone's best interest.

The Malicious

Those who do not like your organization or someone working there, for whatever reason, fall into this category. Also, competing organizations may indirectly sponsor malicious activities using third parties. Thus, the malicious may be someone paranoid, a former employee, a competitor, a terrorist, or, often, simply an angry person. The malicious category also may include the truly delusional, someone, for example, who proclaims the evils of the organization they are attacking in an exaggerated fashion. Needless to say, it is very difficult to reason with such people, who typically enjoy toying with you and amplifying your fear about what they have done or will do.

As when dealing with the attention seeker, you do not want to be openly provocative with malicious attackers, nor do you want them to see you panic. This is the reaction they're hoping for. The best tactic is to distract them so that they believe you are taking a direction that leaves them safe and undetected while, in fact, you are working to get closer to them.

You may never have the opportunity to confront a hacker directly, though the opportunity presents itself far more frequently than you might expect. Most communication will be in the form of anonymous email, an Internet relay chat (IRC), or a phone call. And note that the way you change your system configurations in response to an attack or the manner in which you electronically track an attacker can also be considered forms of communication on your part.

The Curious

Not necessarily seeking attention or intending to cause damage, the curious like to poke around in others' systems and often leave a "trail"; their presence highlights various security holes. The danger presented by the curious type, as with all those who attack your system, is that you're never quite sure what they have seen or done. Their intent isn't clear at first (if ever) because they do not seek attention nor do their exploits reflect any particular objective; often they do not like to talk. And when you study their behavior, you cannot tell whether they have malicious intent or theft in mind; and you are, therefore, left in the frustrating state of not knowing exactly what they are up to.

When dealing with the curious, I attempt to find out what made them curious in the first place and then develop a plan of action accordingly. If you get the opportunity to communicate with them directly, be casual about it. Do not approach them in an aggressive and threatening manner as, chances are, you will not accomplish anything constructive.

The Thief

The motivations of the thief are pretty clear, and for that reason thieves are easier to profile from a behavioral standpoint. Unfortunately, they are, in general, also significantly more skilled at going unnoticed, getting what they are after, and covering their tracks. They are adept at various methods of breaking system security and often possess greater levels of interpersonal skills than the other categories of hackers. And they are better than most at so-called social hacking (for example, calling on the phone to gain information useful in their hacking endeavor).

If thieves are caught, they may try to con you by masquerading as one of the other forms of hackers (the curious or the attention seeker). More often than not, they leave only faint traces that they've been present with nothing to lead you to them. Thieves are often professionals, and most organizations are in over their heads when trying to deal with them. Many organizations also put themselves at a disadvantage by failing to acknowledge that paid "hired guns" are going after their information and infrastructure. This is a mistake.

The Unintentional Hacker

Security holes are often introduced accidentally by someone working within or on behalf of your company. Often their accidents resemble the footprints of one of the other types of hackers. Unrealistic and difficult-to-manage security policies can render an organization accident-prone because individuals naturally skip steps and work to bypass overly complex security policies and procedures. Security measures must not introduce so many details as to cause them to be ignored or otherwise implemented improperly by someone whose job is not security, but the organization's mainline business. This is why the security planning process must consider the business process needs of the organization. Security measures developed in absence of an understanding of an organization's business processes are inherently problematic.

Negotiating with Hackers

As I touched on in the preceding descriptions of the types of hackers, you cannot afford to take the perspective that all hackers are bad people and, if and when you communicate with one of them, that your objective should be to try to intimidate them and prosecute them maximally. This mind-set runs counter to the nature of the problem. There will always be hackers; you cannot stop them. Yes, you must deal with them, but to do so successfully, you need to understand them and learn to handle them with finesse, which doesn't mean immediately poking out your chest and starting a fight. Generally, you have more of an opportunity to communicate civilly with hackers than you realize. The best way to promote communication with a hacker is to provide an easily identifiable email address such as security@yourorganization.com on your Web site for anyone to email security concerns. For example, you can put a link to this address on your Contact Us or similar Web page. You need to make someone responsible for conscientiously sifting through these emails for real security issues and for answering them. In my experience, for every one email having something to do with security, you'll receive 500 that do not. For those that do, the information you learn will be invaluable. Also, if your company provides products and maintains a customer support interface (phone, Web form, or email), the customer support staff should be told to forward concerns from customers about security to a designated point of contact. Make sure the people handling these security inquiries take the task seriously and are trained well enough to know when to escalate a security concern. There's no better way to anger hackers than to ignore their efforts at trying to help you. Typically, they respond by redoubling their effort to embarrass you.

Again, not all hackers are bad; they don't all have malicious intent. And even if you are dealing with one that does, do you really want to anger him or her before you have the situation under control? Remember, these are people who thrive on the feeling of power they get from hacking. Your rage only motivates them further.

A company I was once associated with made the headlines sometime after I left by taking an aggressive tack against a hacker who was attempting to extort money from it. The company poked their chest out and became very confrontational with the hacker. In fairness, some hackers simply cannot be dealt with in a rational manner. But it's always best to try to do so initially. For example, it may seem that the hacker wants money, but, in fact, it's often attention and notoriety. The point is, you need to be sure you know what it is they want. Consider all of your options *calmly,* balanced against the risks. The presumption here is that you are vulnerable in some way and that they have some level of expertise in that area. If you look at it that way, the picture may change from one of a stand-off to a process of learning and negotiation.

The truth is that against the best hackers, especially the hired guns with criminal intent, the best offense is a good defense, in form of a solid security implementation, as described in this book.

STEALING YOUR CREDIT

According to *The Washington Post* (May 17, 2002), credit reports of 13,000 wealthy people were stolen from the credit-reporting company Experian's database by intruders posing as Ford Motor Credit employees. These private credit reports could allow the intruders to run up large balances on existing credit card accounts or to open up new ones in the victims' names. Federal Trade Commission officials and computer database experts said they'd never heard of anyone stealing so many key identities from a credit-report provider, the sort of company generally believed to have very tight security.

Selling Security

Remember I said earlier that we need to *sell* security, not force-feed it to an organization? To sell security successfully—that is, to achieve *buy-in*—you first must have a clear understanding of how people typically solve problems in general. Consider these basic observations as they relate to an organization's executive staff, middle management, and staff members:

Executive management. Executive managers spend money to gain something (as in revenue), to save money (as in cost reduction), or increasingly, to reduce corporate exposure to potentially devastating losses from a security breach. Executive managers today are learning the hard way that a security breach of great-enough magnitude can destroy their company's business (you'll see examples of such breaches throughout this book). Executive managers, by charter, *must* manage the exposure of the organization to these risks. In fact, most managers are quite willing to learn to do so if security planners would communicate their options in terms they understand. Communicating security options effectively is one of the objectives of this book.

Middle management. Middle managers understand processes and procedures that do not impede their main business objectives. Their focus is more on the particular systematic objectives of their department and associated tight schedules. Within the classical corporate organizational structure, middle managers typically do not own the same bottom-line dollar and asset responsibility that executive management does. At the same time, they are typically one step removed from the day-to-day tasks of staff members.

Staff members. The staff understands the task of implementing their day-to-day functions and appreciates changes that help them do their jobs better, but only when these changes are carefully communicated in terms of their day-to-day job description. Conversely, they rebel against corporate overhead of any kind that they don't understand to be a benefit.

Rarely will these groups effectively support anything they cannot relate to on these terms. Herein lies the reason why, historically, organizations have resisted large-scale investment in security systems, processes, and procedures, or if they do invest, why adoption is so poor. If security experts do not fully understand the business, organizational roles, and people in general, they will not make the security sale. Security experts must be educators, which means they must understand human beings outside of their world, because all parties influenced and affected by security (and that's everybody) need to understand, in a balanced fashion and in terms they understand, what security means to them.

We'll consider a simple example of this in a moment, but first let's quickly review authentication, tokens, smart cards, and biometrics to ensure we're all on the same page here.

Authentication, Tokens, Smart Cards, and Biometrics: An Overview

Authentication is the process of validating a user, ensuring that you are who you say you are. Solutions range from traditional username/password regimens to the use of complex devices such as *tokens*, *smart cards*, and *biometric scanners*. A smart card is a specific example of a token.

A system can authenticate you by examining three things: *what you know*, *what you have*, and *what you are*. Not all solutions use all three, though. Tokens (what you have) must be paired with passwords (what you know) or biometric technology (what you are) to produce a stronger solution. This helps prevent the use of stolen tokens.

One popular token design, used in the RSA SecurID card, displays a constantly changing numeric identifier on a tiny LCD screen; the number is synchronized with server software. A user logs on by entering a username, a password, and the identifier currently displayed on the token. The server-side software computes the correct identifier for that token at that moment. Although such tokens improve security, they can be expensive and have a finite battery life. The entire token must be discarded when its batteries expire because its tamper-proof design does not allow for batteries to be replaced. Another type of token called a smart card contains an embedded chip that can be programmed to send and receive data and perform computations. The underlying electronics are small and can be shaped into a wide range of physical packages. Most smart cards are driver's-license- or credit-card-shaped. There are three categories of smart cards:

Memory-only. This kind of smart card is capable of storing and returning information, but no more. Such devices have limited use in network security and are generally relegated to applications such as phone cards, gift cards, and the like.

CPU-based. This device is capable of processing information.

CPU- and crypto-coprocessor-based. This type of smart card is typically tied to a public-key infrastructure (PKI) and sometimes called PKI-enabled smart cards. PKI is a combination of software, services, and encryption technologies that facilitate secure communications and transactions. The only way to get a smart card to perform cryptographic operations is to provide a password or biometric information.

Smart cards offer many benefits but require smart card readers or some other way to interface with your computer. As interfaces like Universal Serial Bus (USB) continue to proliferate, the challenges of deployment will decrease; manufacturers are already integrating the smart cards and USB interfaces into single units and providing simple USB-compatible smart-card readers. Biometric authentication systems capture and store physiological traits, such as those of the finger, hand, face, iris, or retina, or behavioral characteristics, such as voice patterns, signature style, or keystroke dynamics. To gain access to a system, a user provides a new sample, which is then compared with the stored biometric sample. Biometric systems offer great promise in user validation but can, for some environments, be expensive and complicated to administer; this deters many companies from deploying them. If these deterrents can be addressed, the technology offers benefits.

Making the Security Sale: An Example

For our example, we'll suppose that an organization is considering the deployment of tokens to strengthen authentication.

- The executive will be concerned with the dollar cost of the deployment (cost addresses tokens, integration, software, servers, staff time, and any other impact on existing business objectives), so he or she will want to know if any cost-savings benefit or revenue enhancement can be had from the deployment. The executive will also expect a clear explanation of the reduction in exposure (risk of loss) if the deployment is carried out versus if things are left as they are.
- Managers, who are concerned with schedules, processes, and procedures, will be concerned with how to manage the deployment of the tokens and how this effort will affect their existing commitments.
- Employees, who tend to take a nuts-and-bolts view of proposals like this, will want to understand the impact that using this token will have on their performance of their daily tasks. Will it get in the way of doing their jobs? What, if anything, will it add to their daily experience: Will it give them any additional flexibility? Or will it impose greater restrictions?

Now let's evaluate how the three types of "extremist" security planners described earlier might try to sell this proposal:

- The shock-advisors typically will try to sell something like tokens by telling staff that if they don't implement such measures, they will forever be victims of hacking, which potentially could cause the demise of the company. People quickly numb to this argument because their experience dictates that this all-or-nothing view is not the only option.
- The nonplanners will often be cynical about such a proposal because it will require an intensity of focus that they are not accustomed to or not capable of investing.
- The ultra-planners will gridlock the organization by excessively broadening the scope of the "security sell." They will instigate unbounded debates on topics such as token standards and product selection. For example, the ultra-planner may embark on an endless study hyperfocused on the merits of one token design over another and the lack of associated industry standards

Clearly, none of these ways of pitching the smart card token deployment will be successful. A better way, one that considers the audience and their points of view, is delineated in Table 1.1.

Table 1.1 Selling a Smart Card Deployment

INDIVIDUAL	POINT OF VIEW	SECURITY SELL
Executive	Revenue, savings, quantitative exposure	Tokens, particularly smart cards, will enable us to sign documents digitally, rather than sign them by hand. We will also be able to streamline workflow in quantifiable ways. Here are specific processes we will bring to an entirely electronic form: [insert specific implementations]. As we move forward, a combined building entry and computer access token can be deployed, allowing us to save *$X* [insert number] per year per employee, money that would otherwise be spent on building access technology. By strengthening authentication we will reduce our exposure to authentication, and impersonation-based security breaches by *X* percent (later in this chapter, and throughout the remainder of the book, we will learn how to estimate reduction in exposure to security breaches). By administering a single token identity rather than the typical seven passwords that employees must remember, it is estimated that administrative overhead will be reduced by *X* percent, reducing workload by *x* number of work hours per month.
Manager	Commitments, processes, schedules, budgets	Tokens will streamline workflow processes by reducing the number of required passwords that must be administered, from seven on average to just a single identity. This will reduce the time required to grant new employees access to network-based applications to approximately four days on average. Worker efficiency will increase by reducing, on average, three manual steps out of the top five processes carried out by employees. Instead, those steps will be automated through an electronic digital signing process. By reducing exposure to security hacks by *X* percent, risk to schedules caused by the need to respond to such hacks will also be reduced by *X* percent.

INDIVIDUAL	POINT OF VIEW	SECURITY SELL
Staff	Impact on daily tasks	Employees will no longer need to remember and manage an average of seven passwords. Each employee will manage a single identity, the token assigned to him or her. Over time, the same token used for building access and access to employee benefits online will also be used to gain access to other electronic resources. The ability to sign documents digitally and send them electronically, rather than sign them manually and send physical paper, will save time, make everyone's job easier, and make key processes more reliable.

Doing the Math

Once we decide to plan security effectively, it becomes clear that we need a business equation to help us decipher the morass of security problems, challenges, and technology we face in the process. The equation should help us prioritize our (usually scarce) security dollars and resources so that we focus them on the infrastructure that, if hacked, presents the greatest negative impact to our organization. The objective then becomes to implement security solutions that reduce the risk of such a hack occurring.

And because security is not an absolute science, such a business equation will be an approximation, not the result of a formal scientific derivation . Most of us have a very difficult time predicting and estimating things we cannot analytically dissect to the most discrete level of logic. Security risk management, therefore, is somewhat of a challenge. But in the face of as-yet-unknown threats and scarce preventive resources, we must do just that: approximate and predict. Furthermore, we need a risk management business equation tailored specifically to the problem set of security. That's what I introduce here and what we'll use throughout the book: a form of risk analysis tailored to the needs of the security planner and the business needs of the organization. I call it *security impact analysis.*

Understanding Impact Analysis

The first step in developing a security plan is to perform a security impact analysis. This analysis attempts to evaluate the effects of a security breach on your business, so that you can identify the areas of greatest vulnerability. The next step involves developing a sound security implementation, which is driven by your impact analysis, thereby giving you the most bang for the buck.

These two steps are not as straightforward as they might seem, however, because a security breach has several dimensions when it comes to assessing its impact on your business. That is, it's not simply a matter of determining the raw value of information and then predicting how much money you will lose when it's rendered inaccessible, stolen, or destroyed by a hack attack. Consider, for example, that systems offering an opportunity for bad press in a public forum are also very attractive to hackers. Therefore, when evaluating the technical and business impact of a security compromise, you need to consider four important exposure parameters:

Relative value of the information or infrastructure component (V). For example, product plans, accounting systems, customer databases, and so forth typically have a high value, while a company newsletter has a lower value.

Degree of public exposure (P). A defaced Web site, for example, means, at a minimum, embarrassment to a company. This can translate to loss of consumer confidence in an organization's products and services.

Denial-of-business (DoB) potential. Will an attack affect your ability to do business? It's one thing to be inconvenienced, quite another if your ability to operate your business is entirely halted.

Ease of attack (E). The easier a component is to attack, the more often it will be. Components closest to the public Internet are clearly more accessible and, thus, the best first targets. These systems also act as excellent "jumping-off points" for further attacks. Hackers compromise such systems, install their tools on them, and then launch attacks from those systems, perhaps leveraging any preconfigured trusts these systems possess, relative to other components in your infrastructure.

These are the factors to consider when performing a security impact analysis. In a large company, a security team drawn from business and technical areas would likely do the analysis. In a large company, the analysis might be very complex, requiring the team to assess the relative value and vulnerability of dozens of components. (See Chapter 2 for a discussion of the formation and dynamics of a security planning team.)

Performing Security Impact Analysis: An Example

In this section we'll look at these factors within the context of an imaginary company with five key systems. Table 1.2 describes these five systems, and Table 1.3 assigns values (0 through 25) to each of the impact analysis parameters for these systems. A value of 0 means the parameter represents no risk of impact on the organization (no security worries), whereas a value of 25 translates to a maximum impact for that parameter (serious problems may be in store for the company unless changes are made to better protect the environment). Each of the exposure parameters is assigned values based on the current security mechanisms in place within the company. (In this chapter and in Chapter 2, I'll explain how you can organize and conduct meetings to assign impact parameters and perform impact analysis.)

We'll call the sum of these four parameters the *security impact value.* This value is used to help drive our security plan priorities. The maximum impact value is the maximum of the sum of each parameter and is, therefore, 100. An impact value of 100 indicates that the security item needs to be addressed immediately by your security plan; a value of 0 means there is no impact for the security item. A higher impact value, therefore, equates to greater impact on the company should the system be compromised, and thus that security item demands priority positioning in the security planning process. Assigning values in this way enables a company to distribute scarce resources where they are needed most.

WHAT'S IN A NUMBER?

In performing security impact analysis for clients, I have concluded that it helps to keep numbers simple; that is, that they add up to a round, easy-to-understand and -remember number, such as 100. I've seen people become distracted by something as simple as averaging four numbers. In contrast, by taking four variables that add up to 100 in the maximum case, it eliminates the need to compute a simple average. You may be surprised to learn that, over time, people's "gut" takes over, and these impact numbers become surprisingly accurate, as opposed to a number in the range of 1-4 or word values such as "poor," "good," or "excellent." In summary, people are capable of estimating to a better level of granularity using simple numbers—at the same time, they don't want to take out their calculators. Adding four numbers that total to 100 (in the worst case) tends to work best when factoring in the realities of the process and the people involved in that process.

Table 1.2 Five Systems

RISK ELEMENT	DESCRIPTION
Public Web site	Not critical to day-to-day operations. Used for customer support, product information, and investor information.
Mail servers	Used in day-to-day operations by managers and employees. If a mail server is down, business does not stop, but it is hampered.
Accounting systems	Holds all key company financial information, hence is required for the company to do business.
Desktop virus	All employee operations, including manufacturing, can be brought to a standstill if a destructive virus is spread to desktop computer systems in the organization.
Corporate network uptime	This mission-critical internal network connects corporate systems and desktop systems.

As you can see from Table 1.3, the overall impact for our imaginary company is highest (95) for the accounting systems because of high scores on the parameters. The accounting system should, therefore, be the first focus, meaning that the security plan should be developed to reduce accounting system vulnerability.

Table 1.3 Example Impact Analysis

RISK ELEMENT	VALUE OF INFORMATION (V)	PUBLIC EXPOSURE (P)	DENIAL OF BUSINESS (D)	EASE (E) OF ATTACK	OVERALL IMPACT
Public Web site	13	25	5	23	66
Mail servers	23	15	20	18	76
Accounting systems	25	25	25	20	95
Desktop virus	25	15	25	23	88
Corporate network uptime	25	18	25	20	88

Counting the Cost of Security

The security planning process can be realistic only if cost is considered. Not recognizing this is the number-one reason well-intentioned security planning efforts fail. Organizations have finite resources—their budgets, staff, and ability to accommodate security overhead are all limited. Therefore, the objective is to intelligently reduce vulnerability to the lowest acceptable level, minimizing the cost required to do so.

The objective is to avoid throwing all the money you have at the first challenge. Rather, you want to spend money to reduce vulnerability for each of your high-impact systems. After applying your security measures, you revise values for the four exposure parameters for your systems and compute a new impact value, one that is acceptably lower.

For the sake of providing a simplified framework for analyzing cost scenarios for reducing impact based on improved security, we can group the costs of security plan preventive measures into three categories: *low*, *moderate*, and *high*. Each group implies a particular level of security and a corresponding reduction in predicted impact on the company should the component in question be compromised.

Returning to our example, we'll assume the security team met and, using the planning tools provided in this book, developed three potential security solutions intended to reduce vulnerability in the accounting systems:

Low cost. Maximum use of freeware and implementation of good practices. Estimated impact reduction is 35 percent.

Medium cost. Enhanced use of commercial software products with additional security measures and improved vendor support. Predicted impact reduction is 50 percent.

High cost. Enhanced solution with greater diversity, redundancy, and stronger authentication. Impact reduction is 60 percent.

Figure 1.1 illustrates how the analysis might proceed. The vertical axis shows cost; the horizontal axis is the impact value for that given cost solution. The lines dividing the graph into four sections represent maximum allowable impact and cost (these maximum values were selected by the security impact analysis team, a process we'll talk about in a moment). This produces four categories of solutions, as drawn in the figure. Here, the team placed its low-, medium-, and high-cost solutions on the graph. The medium-cost solution was considered the best solution (low vulnerability + acceptable cost).

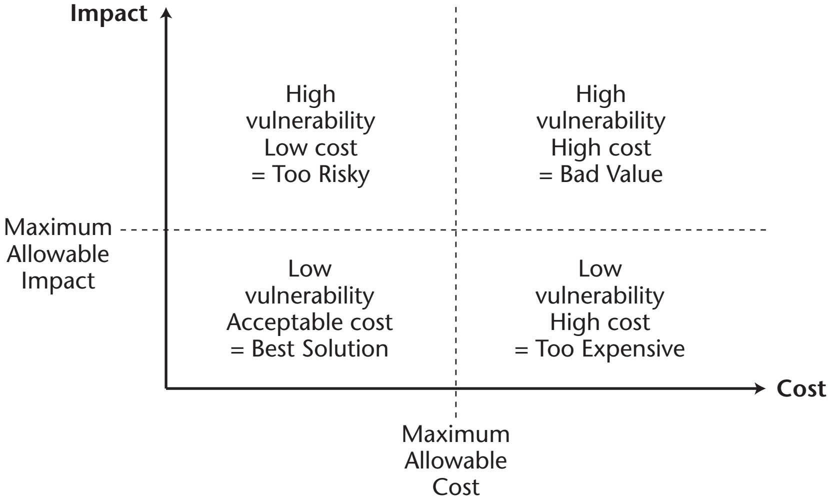
Impact
High vulnerability Low cost = Too Risky
High vulnerability High cost = Bad Value
Maximum Allowable Impact
Low vulnerability Acceptable cost = Best Solution
Low vulnerability High cost = Too Expensive
Cost
Maximum Allowable Cost

Figure 1.1 Impact analysis graph.

Establishing Maximum Impact, Cost, and the Security Budget

As the security team becomes more comfortable with its ability to perform impact analysis consistently and see positive results, its members will gain a better feel for what represents excessive impact to the organization. Eventually, the team will reach a consensus view on what is meant by, for example, an impact value of 75 versus 40. Over time, the team will become comfortable producing guidelines that say, for example, that given the current available security budget, anything with an impact value greater than 75 is not acceptable.

The maximum cost parameter represents the team's consensus view on how much of its budget can be allocated to this particular security item. The cost of security is both relative and absolute. Clearly, the costs of the solutions in our analysis (low, medium, and high) are relative to each other, in that, for example, one may cost $500 while another may cost $50,000 to implement. They are also relative in that if the value of the protected information or infrastructure is very high, arguably more costly security measures are in order. For example, if we allow for a 5 percent protection cost (a total cost for staffing, software, hardware, training, organizational awareness programs, and so forth), then we might accept that information or infrastructure valued at $1 million could easily justify a relative security investment of $50,000. The concept of allocating security dollars based on the value of an asset is directly analogous to the way we buy insurance today. When we insure our home or car, for example, our insurance premiums increase right along with the value of the home or car.

Returning to our example, the cost is absolute in the sense that we must have $50,000 in the bank if we go this route. This whole discussion of relative and absolute costs at first may seem academic; however, when we try to communicate and sell security within our organization, it becomes clear that people, at least subconsciously, think along these lines and that such a thought process can be used to drive their decisions more effectively.

None of this discussion about relative costs, insurance premiums, and so forth is meant to imply that simply throwing dollars at the problem improves security. Intelligence, experience, common sense, and savvy are also important factors in successfully securing systems. But, on average, a well-managed security group that is better funded will do better work and offer improved security. It will have the budget to hire sufficient staff and invest in important security infrastructure software and systems, and it will have the time and money to enforce security policies and procedures and to provide training within the organization.

Estimating the Value of Security

When you do an impact analysis, you are required to make some tough decisions about the value of security. To make those decisions, you must first determine the answers to relevant questions. How valuable are your product plans? How about your company phone directory? (Relative to phone numbers, for example, some companies publish these on the Web, while others view them as highly confidential and would never consider that level of exposure, given that the phone is an excellent tool for social attacks—to gather confidential information from individuals—not to mention that competitors can use your phone directory to attempt to hire your employees away from you.) How might your customers react if your company's Web site was defaced by hackers? If yours is a publicly held company, how might this form of attack affect confidence in your service and products, or in your stock value?

Depending on your company and the type of product or service it offers, everything might be mission-critical, with no shades of gray—the company phone list is as sensitive as your product plans. That said, remember that security planning calls for making tough decisions to control costs and maintain workplace efficiency, which means, in part, avoiding overly cumbersome security processes and procedures. Consequently, someone in your company might need to stand up and say that company phone numbers are important and should be kept confidential, but they're not as security-critical as product plans. Asked to assign a weighting of 0 to 25 (again,where 0 is unimportant and 25 is most sensitive), this individual might assign a 20 to product plans and a 15 to company phone numbers; the company's financial system, crucial to its daily operation, might be assigned a 25.

Laying the Security Foundation

Security policies and procedures define the organization's security-related processes, guidelines, and standards. A procedure might define the process by which an individual in the organization is authenticated and granted access to key applications. A policy might define a standard that requires firewalls from at least two vendors be implemented to protect against a vulnerability in any one vendor's product or that backup filters be resident in all the organization's routers. You will learn more on policies and procedures in the remainder of the book, but for now understand that you must define and maintain them as living documents. In turn, of course, employees also must read and adhere to them. That, then, requires education and an effective security sell. (There's that important verb "sell" again.)

Policies and procedures will be driven by your impact analysis; that is, when you know you might have a lot to lose, it becomes evident that defining policies and procedures to prevent such a loss is essential. Keep these important points in mind as we proceed:

- Publish procedures and policies to all affected people.
- Give appropriate staff members "ownership" responsibility for implementation and oversight of policies and procedures.
- Policies and procedures grow with the organization. They must be kept up to date by accountable staff members to reflect that growth.
- Establish clear accountability and define metrics, to ensure that policies and procedures are followed (you will be given a framework for these metrics later).
- Gather, on a regular basis, input from staff members, always with an eye to improving policies and procedures.

A real-life example is in order here. Consider a grocery store in the United States just beginning the process of installing an auto-checkout capability. With it, customers will be able to check themselves out after selecting their food items, without the help of a clerk behind a cash register. A friend of mine, interested in this installation, noted that the grocery store had wisely implemented a thumbprint biometric scan as part of the registration process. Customers would use their thumbprint cards at the checkouts, where computers would check the cards and thumbprints before automatically authorizing payment from a credit card. This gave my friend a "warm fuzzy feeling" about the process, and he decided to sign up. Part of the sign-up process involved revealing highly personal information, the kind an attacker could use to steal your identity (Social Security number, driver's license number, name, address, and historical information). My friend entered his personal information directly into a workstation set up at the store, provided his thumbprint, and went home.

At home, he realized he had left his driver's license at the store. Upon returning to the store, as he walked over to the enrollment workstation, he noticed that a store clerk had printed his application for manual processing, complete with all his private information, and the clerk had *left it on a desk in the middle of the store*. Needless to say, my friend wasn't very happy. The clerk attending the workstation either hadn't been trained in the *policies and procedures* associated with the process or had none to guide him in the first place.

The result? The security of this customer registration process for auto-checkout, complete with a thumbprint scan, was greatly diminished by the absence of or lack of adherence to security policies and procedures. Clearly, if we're going to spend time, money, and effort to implement security technologies, we need to be sure to implement the policies and procedures that will make them effective in practice.

Improving Security as Part of the Business Process

Throughout the remainder of this book, we will employ an approach to security planning that is as much about business process improvement as it is about technology. We will work to understand our organization, our policies, and our procedures; and we will measure the cost and effectiveness of our security planning effort by defining appropriate measures (metrics) and a means of tracking and analyzing them.

Like business process improvement, security demands that we address the relationship of people to our processes and procedures. When we define a security process, we define a *process owner*. We present a method for streamlining our security and for continuously improving it. Very importantly, our security plan addresses education, training, and the selling of security to people and their organizations. The entire approach is summarized in Figure 1.2.

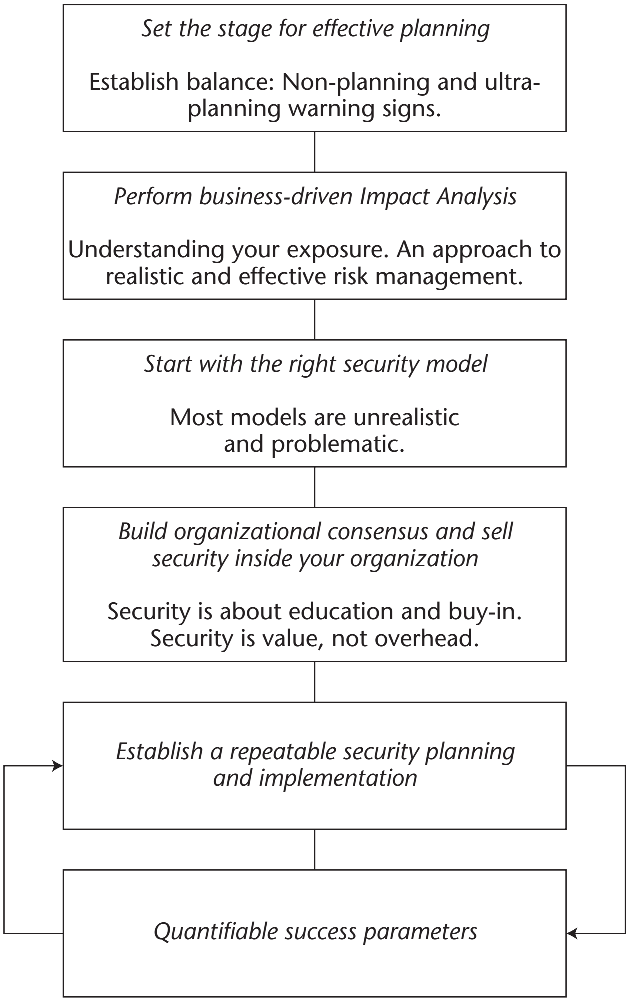
Set the stage for effective planning
Establish balance: Non-planning and ultra-planning warning signs.
Perform business-driven Impact Analysis
Understanding your exposure. An approach to realistic and effective risk management.
Start with the right security model
Most models are unrealistic and problematic.
Build organizational consensus and sell security inside your organization
Security is about education and buy-in. Security is value, not overhead.
Establish a repeatable security planning and implementation
Quantifiable success parameters

Figure 1.2 Security is business process improvement.

Conclusions

This chapter laid the groundwork for our planning approach, essentially defining the fundamental staples of security planning. We now have at our disposal a way to prioritize and focus our goals: We have gained a perspective on balanced security planning; we have the beginnings of an approach to selling security; and, finally, we have the framework for a security business improvement model. We will put all of this to work in future chapters, starting in Chapter 2, where we address forming a security planning team and developing a detailed security planning template.