2

Why You Can Never Be Secure

The title of this chapter seems to directly contradict the message of the book; however, it is accurate. It's true that you can never be 100 percent secure. The only people who claim they can provide you with complete security are fools or liars.

However, you can be secure enough. That is the key principle. You will always have an element of risk in everything you do. The only way to avoid risk is to not do anything. (But consider that if you sit at home locked in your room, a meteor can strike your house or an electrical fire can start.) In reality, people and companies cannot avoid risk. The only way to not assume risk is not to do business.

Unfortunately, companies and people tend to ignore all risk and charge ahead. For example, many companies want to do business on the Internet because of all the potential financial benefits. However, they ignore the fact that there are dangers, or risks, that incur costs they are not familiar with. Frequently these quick movers think they are too small for anyone to want to attack them. As you should know from reading the previous chapter, this company is now the perfect victim. Companies want the benefits without acknowledging the costs.

Would a business buy a delivery truck and not get insurance or fail to maintain that truck? Of course not, because it presents too much risk, and it just goes against all notions of common sense. People know

that there is a cost to pay to get the potential benefit of having a delivery truck. However, people completely ignore this concept when it comes to the Internet and computers in general.

The Risk Equation

The core of the intelligence process, described in Chapter 1, is compromising vulnerabilities and avoiding countermeasures in the pursuit of valuable information. It's about determining needs and satisfying them. Another word for this process is *espionage.* When a company is the target of intelligence activities, the process is called *industrial espionage.* The chances that an intelligence operation will breach your company's security and compromise something valuable is called *risk.*

Risk is the driving consideration of all corporate espionage activities. The strategic decisions of those who would attack your organization are driven by it; the types of counterintelligence measures, or security countermeasures, you put into place depend on it. You can't take appropriate steps to protect your personal information without first understanding the concept of risk.

In emotional terms, most people think of risk as their chance of experiencing pain. They manage their risk by balancing their chances for pain against their chances for pleasure. Unfortunately, many organizations base their corporate risk management decisions on emotion rather than on sound research. "It wouldn't happen to me" or "I have nothing that anyone would want" are all-too-common beliefs floating around the business world, with no solid foundation. This head-in-the-sand attitude increases the risk to companies of all sizes, leaving them vulnerable to major losses.

The other extreme is to overreact—to spend money on trendy countermeasures that are not appropriate and deplete resources without reducing risk at a reasonable cost. It doesn't make sense to spend more money and effort protecting information than the information is actually worth.

The post-September 11 hysteria is an example of inappropriate risk management. People ran out and bought gas masks. Somebody even bought enough plastic sheets and duct tape to seal his entire

house. The news media rushed to the middle of nowhere to feature this idiot. So what's wrong with these countermeasures?

Gas masks provide protection against gas attacks. They are basically useless against most real chemical and all biological attacks. You actually need a whole suit for that. Also, gas attacks are a significant threat only in closed spaces, yet most people who bought gas masks didn't take them along to their visits to such places; most kept their masks at home. So gas masks sound good but do little to save a life even in the most likely attacks.

Plastic sheets and duct tape are a countermeasure to potential biological and chemical attacks. However, those types of attacks are usually limited to a very small area. The likelihood of some terrorist targeting farm country to attack the person who covered his whole house was infinitesimal at best. At the very least, this irrational act attracted attention to the person in the first place, which put him at greater risk. More likely, he would suffocate himself and his family because no fresh air could come into his house.

Fortunately, you can disregard the hype and madness and use a scientific way to define your personal and organizational specific level of risk. This formula, called the *risk equation*, has been used by statisticians to establish insurance-related risks for decades. The risk equation (shown in Figure 2.1) includes four essential components: value, threat, vulnerability, and the countermeasures.

$$\text{Risk} = \left(\frac{\text{Threat} \times \text{Vulnerability}}{\text{Countermeasures}} \right) \times \text{Value}$$

Figure 2.1 The risk equation

- **Value.** This refers to the worth of your information or other assets, both monetary and otherwise. The value of your information must temper the funding and allocation of your espionage countermeasures. You don't want to spend more money, time, and effort protecting your information and other resources than it would cost you to lose them. For example, you would not normally pay $3,000 to install a car alarm on a $2,000 vehicle. However, multibillion-dollar corporations cannot protect billions of dollars' worth of information with less than a million-dollar security budget (although many firms have tried). Chapter 3 discusses how to determine the value of information.

- **Threat.** Simply put, threat refers to the people, organizations, and other entities who might be after your valuable resources. A threat can be intentional or inadvertent, manufactured or naturally occurring. Although companies do not always want to acknowledge it, there is always a threat in one form or another. Chapter 4 describes how to identify threats.
- **Vulnerability.** This refers to your organization's weaknesses or what allows a threat to exploit you. If you have no vulnerabilities, a threat cannot exploit you, so you have no risk. Computers connected to the Internet, unlocked offices, employee ignorance, spotty security procedures, and putting a building in a flood zone are examples of vulnerabilities. Vulnerabilities can never be wholly removed from an organization, but they can be managed with countermeasures. Chapter 5 examines vulnerabilities.
- **Countermeasures.** These are the steps, procedures, and devices that you have in place to address your specific vulnerabilities. If your organization establishes a set of countermeasures that fails to address your vulnerabilities, you're just wasting your money. An awareness program that leaves out certain weaknesses in your organization does nothing at all to plug those holes. See Chapter 12 for an extensive list of countermeasures.

All these components affect one another. It is their interaction that determines your risk level. If, for example, you accidentally leave a piece of paper in the public library, the information on that piece of paper is highly *vulnerable.* You have to assume that your competitors are interested in everything about your company, so there is a *threat* that someone wants to find that paper and use it against you. If, however, that paper contains only widely available information—say, the address of your company—it wouldn't have much *value* to a competitor. Consequently, you create *zero risk* to yourself or your business from this piece of paper. Paying a security guard to protect that scrap of paper would not be an appropriate *countermeasure*.

The Risk Assessment Process

Mathematical models of security-related risk can be very useful to a wide range of organizations. Big companies are familiar with creating such models for nearly every business decision, but the process might

be new to smaller operations and individuals. Smaller organizations and individuals can step through the process intuitively, without assigning numerical values.

Say that your company is a small manufacturing firm. You have developed a new process for producing a special gear at much less cost than your competitors can produce it. This gear can greatly increase your sales and profits, and it could do the same thing for your competitors if they knew your process. Also say that many other companies produce this particular part. Clearly, you have a threat to your organization that could be called medium to high. Also, you have identified weaknesses in your operation, but not a huge number of them, so your vulnerability is medium. You have high value, medium to high threat, medium vulnerability, and no real countermeasures. Your risk would be medium to high, and you should increase your countermeasures as appropriate, based on the vulnerabilities that are most likely to be exploited.

From the Spy's View

Industrial spies—one of your threats—also use a version of the risk equation. The risks involved in any one information-collection action influence the choice of collection methods. The collection of highly vulnerable information usually involves little risk. The collection of very valuable information, even though it is protected by extreme countermeasures, may warrant a high level of risk.

At one extreme, spies may choose to kidnap an executive to secure extremely valuable and inaccessible information as ransom. Most targets, however, do not warrant such a risky operation or such an enormous expenditure of resources.

Spies also weigh the costs of detection against the possible benefits of securing the information. Unfortunately, most spies face very few effective countermeasures, so *their* risk is often quite low.

What Is a Security Program?

The risk equation actually defines the goal of a security program. Consider that you do not have any control over the assessment of the value, threat, and vulnerability of your organization. In fact, you and your

organization want to increase your value as much as possible, which increases your risk as a whole.

No individual security program can completely remove a threat. You cannot get rid of people who want to harm you. You cannot stop an earthquake or a flood from occurring. The United States has still not wiped out terrorism, despite all its resources.

Vulnerabilities will always exist as well. As long as you function in the real world, vulnerabilities can't be avoided.

Your security program is the implementation of countermeasures to address the vulnerabilities. Value justifies the amount of money you spend on the program. Defining the threat helps you determine the vulnerabilities that are most likely to be exploited, as well as the scope of resources the threat may use against you.

Risk Optimization

Only when you understand the real components of risk can you put together an effective and appropriate strategy for protecting your organization and managing your risk. By addressing your vulnerabilities and *optimizing*, rather than *maximizing*, your counterespionage efforts, you can greatly improve your security.

So the goal of your security program is to optimize risk, never minimize it. This is an extremely important distinction. It also sounds counterintuitive to many people.

Think about the meaning of the word *minimize*. The definition is to reduce risk as much as possible, which means that you want to eliminate all possible ways to lose information or other assets. However, a policy that says you need to minimize your risk means that you need to address all risk that you possibly can. That is not realistic from a value perspective.

Consider an automobile. Everyone wants a safe car, but do you want to minimize all risk associated with the car? You can, for example, install more safety equipment. You can be like NASCAR drivers and have a seatbelt that buckles down your entire body. You can install bulletproof glass. You can put a regulator on the car that prevents it from going faster than 30 miles per hour. All that would make the car safer. But would it leave the car usable and affordable to most people? Clearly not.

The Cost/Risk Relationship

Figure 2.2 graphically depicts the cost/risk relationship. The vertical edge of the graph represents cost. The curved line that starts in the bottom-left corner represents the countermeasures you implement for your security program. The curved line that starts at the top left represents your vulnerabilities. The area under the vulnerabilities graphically represents your risk or, more accurately, your potential loss.

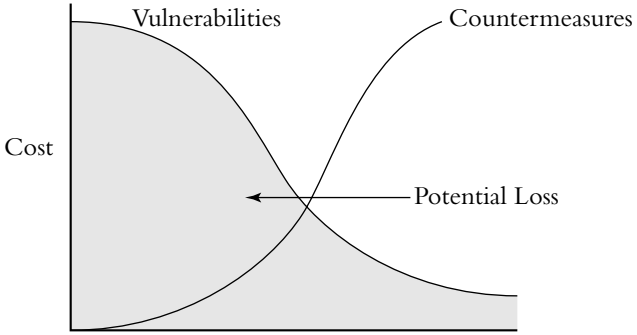

Figure 2.2 The cost/risk relationship

As shown in Figure 2.2, as you start to spend money on countermeasures, risk starts to decrease quickly. Many countermeasures are very inexpensive and have a huge payback. At some point, the vulnerabilities are more difficult and expensive to address, so the payback, or reduction of vulnerabilities, begins to level off.

The graph can extend infinitely to the right. Because you can never have perfect security, the vulnerability line is asymptotic and never hits zero. At the same time, the cost to continue to reduce vulnerabilities, and therefore risk, constantly increases. What is the right balancing point of the cost of countermeasures versus risk? This is risk optimization.

The Balancing Point

Risk optimization is the point at which you appropriately balance the money you spend on your countermeasures, or your security program, with the amount of risk you are willing to accept. Figure 2.3 depicts that point.

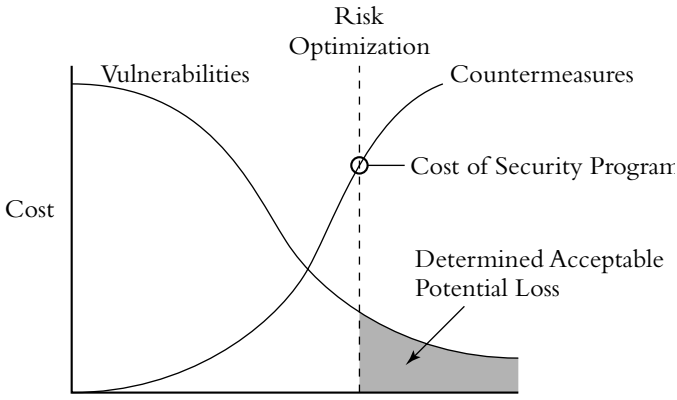

Figure 2.3 Risk optimization

The vulnerability and countermeasure lines are the same as in Figure 2.2. The new vertical line represents a point at which you have balanced the cost you are willing to spend with the amount of risk you are willing to allow to exist in your life or organization.

The point at which the vertical line crosses the countermeasure line is specifically the amount of money being spent. The shaded area below the vulnerability line and to the right of the new vertical line represents the amount of risk you assume by spending that money.

People immediately want to assume that the point of risk optimization is where the countermeasure and vulnerability lines cross in this graph. That is incorrect. The appropriate way to optimize risk is to first determine the amount of risk you are willing to accept. Figure out how big of a shaded portion remains. Again, the value you protect should assist in determining an acceptable level of risk. At that point, you determine the cost for implementing the countermeasures you need to be left with that amount of risk. This should be the decision process.

There is another reason that the point where the countermeasures and vulnerabilities cross is not a good way to choose the amount of risk you are willing to accept. In all but extreme examples, you do not want to invest more money in your countermeasures than the amount of remaining risk. It is not cost effective. Likewise, Figure 2.3 is not a situation that most businesses would implement, for which the money invested in a security program is more than the remaining risk. The optimization point is drawn there only for the sake of clarifying the graph.

Unfortunately, people and companies always seem to first choose how much money they want to spend on their countermeasures (security program), without considering the amount of risk they can accept. The amount of risk you or your company accepts should be a conscious choice.

One question people frequently ask me is, "What percent of my budget should be allocated to security?" I really hate that question, because it demonstrates an ignorance of risk. A security program budget should be determined by examining where your security program needs to be, where you are now, and then how you will get to where you need to be. If you already have a good security program in place, you just need a budget to maintain that level of security. If, however, your security program is lacking, it will cost you more, because you need to spend money to bring your security program up to par. Whatever that costs is how much you must spend to leave only that amount of risk you consciously decide is acceptable.

The concepts here are valid for security programs as a whole, as well as for information security programs.

Risk Optimization in Action

It is extremely difficult to determine an appropriate security budget, even when you are implementing a risk optimization thought process. At a high level, you can look at your potential loss and attempt to determine an appropriate level. For example, if you are in a bank that performs billions of dollars of transactions a day, that is your potential loss. You may then figure out the likelihood of loss, and multiply that by the dollar value of the potential loss. For example, a bank performs $6,000,000,000 of transactions per day. If you assume that there is a .1 percent likelihood of a serious incident, and that there are approximately 250 trading days per year, the overall potential loss is $6,000,000,000 × 250 × .001, or $1,500,000,000 annually. It is therefore not unreasonable for a bank to have a security budget of more than $100,000,000 annually.

At a personal level, consider a home that has $20,000 of belongings. If the owners have insurance with a deductible of $1,000, they have a potential monetary loss of $1,000. It may also be reasonable to

include nuisance value to add to potential loss, which you can estimate at $10,000. This means that your potential loss is $11,000. If you assume that the likelihood of experiencing a loss is 3 percent, the estimated loss is $330. Is it therefore logical to add an extra lock on your front door for $50? Or, $300 for a home alarm monitoring service? Clearly there is a psychological component to add to these calculations; however, from a strictly financial perspective, the single lock is a much more reasonable investment than the home monitoring service.

In a more reasonable business scenario, it is best to examine vulnerabilities one at a time. For example, you may decide that losses due to poor passwords cost a large organization more than $10,000,000 per year. You determine that the best countermeasure is an "identity management system." The identity management system costs $1,000,000, and will last three years, for an amortized cost of $333,333 per year. That is a reasonable countermeasure to implement.

Chapter 13 thoroughly discusses implementing risk optimization.

Conclusion

Notice that what I'm talking about in this chapter is *risk management*. Companies functioning in the real world will never be totally risk free. Enterprises must exchange information with employees, suppliers, support organizations, the government, and customers on a daily basis. You can't do business in a vacuum.

Fortunately, you don't need to seal your company in a bubble to keep your information safe. Many highly effective countermeasures are simple, inexpensive, and not particularly disruptive of your day-to-day operations. People are surprised when they learn that the simplest countermeasures often provide the greatest protection.

This does not mean that you should spend little on your security program. The amount you spend must be a conscious decision based on the amount of risk you want to accept.

My editors commented that this chapter seems "light." From a size perspective, that is true. However, from a content perspective, this is the most valuable chapter in the book. When you truly understand the concept of optimizing risk and making a purposeful decision to accept risk, you can actually implement a proactive security program.