Part One

Sensible Security

Chapter 1

All Security Involves Trade-offs

In the wake of 9/11, many of us want to reinvent our ideas about security. But we don't need to learn something completely new; we need to learn to be smarter, more skeptical, and more skilled about what we already know. Critical to any security decision is the notion of trade-offs, meaning the costs—in terms of money, convenience, comfort, freedoms, and so on—that inevitably attach themselves to any security system. People make security trade-offs naturally, choosing more or less security as situations change. This book uses a five-step process to demystify the choices and make the trade-offs explicit. A better understanding of trade-offs leads to a better understanding of security, and consequently to more sensible security decisions.

The attacks were amazing. If you can set aside your revulsion and horror—and I would argue that it's useful, even important, to set them aside for a moment—you can more clearly grasp what the terrorists accomplished.

The attacks were amazing in their efficiency. The terrorists turned four commercial airplanes into flying bombs, killed some 3,000 people, destroyed $40 billion in property, and did untold economic damage. They altered the New York skyline as well as the political landscape of the U.S. and the whole world. And all this was done with no more than a thirty-person, two-year, half-million-dollar operation.

The attacks were amazing in the audacity of their conception. No one had ever done this before: hijack fuel-laden airplanes and fly them into skyscrapers. We'll probably never know for sure if the terrorists counted on the heat from the ensuing fire to fatally weaken the steel supports and bring down the World Trade Center towers, but those who planned the attacks certainly chose long-distance flights as targets, since they would be carrying heavy fuel loads. The scheme's audacity meant no one had planned a defense against this type of attack.

The attacks were amazing for their detailed planning and preparation and the discipline shown by the multilayered, compartmentalized organization that carried them out. The plan probably involved a total of some thirty people, and, of these, some had to have been willing to die. Others most likely had to be kept from knowing they were going to

die. The keeping of secrets and careful parceling out of information doubtless required training. It required coordination. It required extraordinary discipline. Indeed, the sheer scope of the attacks seemed beyond the capability of a terrorist organization and in fact has forced us to revise our notions of what terrorist organizations are capable of.

At the same time, the entire operation was amazing in its technological simplicity. It required no advanced technology that couldn't be hijacked or (as in the case of GPS devices) easily purchased. All technical training could be easily had. And there was no need for complex logistical support: Once the attacks were set in motion, the terrorists were on their own; and once they were in the air, each group of four or five was on its own, independent and self-sufficient.

The attacks were amazing because they rewrote the hijacking rulebook. Previous responses to hijackings centered around one premise: Get the plane on the ground so negotiations can begin. The threat of airplane bombings, we had come to believe, was solved by making sure passengers were on the same flights as their baggage. These attacks made all that obsolete.

The attacks were amazing because they rewrote the terrorism book, too. Al Qaeda recruited a new type of attacker. Not the traditional candidate—young, single, fanatical, and with nothing to lose—but people older and more experienced, with marketable job skills. They lived in the West, watching television, eating fast food, drinking in bars. Some vacationed in Las Vegas. One left a wife and four children. It was also a new page in the terrorism book in other ways. One of the most difficult things about a terrorist operation is getting away at the end. This suicide attack neatly solved that problem. The U.S. spends billions of dollars on remote-controlled precision-guided munitions, while all Al Qaeda had to do was recruit fanatics willing to fly planes into skyscrapers.

Finally, the attacks were amazing in their success rate. They weren't perfect; 100 percent of the attempted hijackings were successful, but only 75 percent of the hijacked planes successfully reached their targets. We don't know if other planned hijackings were aborted for one reason or another, but that success rate was more than enough to leave the world shocked, stunned, and more than a little bit fearful.

• • • •

The 9/11 terrorist operation was small, efficient, relatively low-tech, very strictly disciplined, highly compartmentalized, and extremely innovative. Did we stand a chance?

The plan's size, discipline, and compartmentalization were critical in preventing the most common failure of such an operation: The plan wasn't leaked. Al Qaeda had people in the U.S., in some cases for years, then in staged arrivals for months and then weeks as the team grew to full size. And, throughout, they managed to keep the plan secret. No one successfully defected. And no one slipped up and gave the plan away.

Not that there weren't hints. Zacarias Moussaoui, the "twentieth hijacker," was arrested by the FBI in Minnesota a month before the attacks. The local FBI office wanted to investigate his actions further. German intelligence had been watching some parts of the operation, and U.S. and French intelligence had been watching others. But no one "connected the dots" until it was too late, mostly because there really were no dots to connect. The plan was simply too innovative. There was no easy-to-compare template and no clear precedent, because these terrorists in a very real sense wrote the book—a new book.

Rarely does an attack change the world's conception of attack. And yet while no single preparation these terrorists made was in and of itself illegal, or so outlandish that it was likely to draw attention—taken together, put together in just this way, it was devastating. Nothing they did was novel—Tom Clancy wrote about terrorists crashing an airplane into the U.S. Capitol in 1996, and the Algerian GIA terrorist group tried to hijack a plane and crash it into the Eiffel Tower two years before that—yet the attack seemed completely new and certainly was wholly unexpected. So, not only did our conception of attack have to change; in response, so did our conception of defense.

• • • •

Since 9/11, we've grown accustomed to ID checks when we visit government and corporate buildings. We've stood in long security lines at airports and had ourselves and our baggage searched. In February 2003, we were told to buy duct tape when the U.S. color-coded threat level was raised to Orange. Arrests have been made; foreigners have been deported. Unfortunately, most of these changes have not made us more secure. Many of them may actually have made us *less* secure.

The problem is that security's effectiveness can be extremely hard to measure. Most of the time, we hear about security only when it fails. We don't know how many, if any, additional terrorist attacks were prevented or aborted or scared off prior to 9/11. We don't know what, if anything, we could have done to foil the 9/11 attacks, and what addi-

tional security would have merely been bypassed by minor alterations in plans. If the 9/11 attacks had failed, we wouldn't know whether it had been because of diligent security or because of some unrelated reason. We might not have known about them at all. Security, when it is working, is often invisible not only to those being protected, but to those who plan, implement, and monitor security systems.

But it gets even more complicated than that. Suppose security is perfect, and there are no terrorist attacks; we might conclude that the security expenditures are wasteful, because the successes remain invisible. Similarly, security might fail without us knowing about it, or might succeed against the attacks we know about but fail in the face of an unforeseen threat. A security measure might reduce the likelihood of a rare terrorist attack, but could also result in far greater losses from common criminals. What's the actual risk of a repeat of 9/11? What's the risk of a different but equally horrific sequel? We don't know.

In security, things are rarely as they seem. Perfectly well-intentioned people often advocate ineffective, and sometimes downright countereffective, security measures. I want to change that; I want to explain how security works.

Security is my career. For most of my life, I have been a professional thinker about security. I started out focusing on the mathematics of security—cryptography—and then computer and network security; but more and more, what I do now focuses on the security that surrounds our everyday lives. I've worked for the Department of Defense, implementing security solutions for military installations. I've consulted for major financial institutions, governments, and computer companies. And I founded a company that provides security monitoring services for corporate and government computer networks.

Since the attacks of 9/11, I have been asked more and more about our society's security against terrorism, and about the security of our society in general. In this book, I have applied the methods that I and others have developed for computer security to security in the real world. The concepts, ideas, and rules of security as they apply to computers are essentially no different from the security concepts, ideas, and rules that apply, or should apply, to the world at large. The way I see it, security is all of a piece. This attitude puts me, I suspect, in a minority among security professionals. But it is an attitude, I believe, that helps me to see more clearly, to reason more dispassionately than other security professionals, and to sort out effective and ineffective security measures.

This book is about security: how it works and how to think about it. It's not about whether a particular security measure works, but about how to analyze and evaluate security measures. For better or worse, we live in a time when we're very likely to be presented with all kinds of security options. If there is one result I would like to see from this book, it is that readers come away from reading it with a better sense of the ideas and the security concepts that make systems work—and in many cases not work. These security concepts remain unchanged whether you're a homeowner trying to protect your possessions against a burglar, the President trying to protect our nation against terrorism, or a rabbit trying to protect itself from being eaten. The attackers, defenders, strategies, and tactics are different from one security situation to another, but the fundamental principles and practices—as well as the basic and all-important ways to *think* about security—are identical from one security system to another.

Whether your concern is personal security in the face of increasing crime, computer security for yourself or your business, or security against terrorism, security issues affect us more and more in our daily lives, and we should all make an effort to understand them better. We need to stop accepting uncritically what politicians and pundits are telling us. We need to move beyond fear and start making sensible security trade-offs.

••••

And "trade-off" really is the right word. Every one of us, every day of our lives, makes security trade-offs. Even when we're not thinking of threats or dangers or attacks, we live almost our entire lives making judgments about security, assessments of security, assumptions regarding security, and choices about security.

When we brush our teeth in the morning, we're making a security trade-off: the time spent brushing in exchange for a small amount of security against tooth decay. When we lock the door to our home, we're making a security trade-off: the inconvenience of carrying and using a key in exchange for some security against burglary (and worse). One of the considerations that goes into which car we purchase is security against accidents. When we reach down at a checkout counter to buy a candy bar and notice that the package has been opened, why do we reach for another? It's because a fully wrapped candy bar is a better security trade-off, for the same money, than a partially wrapped one.

Security is a factor when we decide where to invest our money and which school to send our children to. Cell phone companies advertise security as one of the features of their systems. When we choose a neighborhood to live in, a place to vacation, and where we park when we go shopping, one of our considerations is security.

We constantly make security trade-offs, whether we want to or not, and whether we're aware of them or not. Many would have you believe that security is complicated, and should be best left to the experts. They're wrong. Making security trade-offs isn't some mystical art like quantum mechanics. It's not rocket science. You don't need an advanced degree to do it. Everyone does it every day; making security trade-offs is fundamental to being alive. Security is pervasive. It's second nature, consciously and unconsciously part of the myriad decisions we make throughout the day.

The goal of this book is to *demystify* security, to help you move beyond fear, and give you the tools to start making sensible security trade-offs. When you're living in fear, it's easy to let others make security decisions for you. You might passively accept any security offered to you. This isn't because you're somehow incapable of making security trade-offs, but because you don't understand the rules of the game. When it comes to security, fear is the barrier between ignorance and understanding. To get beyond fear, you have to start thinking intelligently about the trade-offs you make. You have to start evaluating the risks you face, and the security options you have for dealing with those risks. There's a lot of lousy security available for purchase and a lot of lousy security being imposed on us. Once you move beyond fear and start thinking sensibly about trade-offs, you will be able to recognize bad or overpriced security when you see it. You will also be able to spot ineffectual security—and explain why it's ineffectual.

As citizens, sometimes we have choices in our security trade-offs and sometimes we don't. Much security is imposed on us by law or business practice, and even if we dissent we cannot choose not to comply with the trade-offs. We cannot opt out of the FBI database, or decide that we would rather not have ourselves recorded on the thousands of security cameras in any major city. Still, there are limited trade-offs we *can* make. Banking security is what it is; we can't choose more or less of it. But we can choose to place our money elsewhere. Airline security is largely dictated by government regulations; airlines don't compete with each other based on security. But we can decide to drive instead. Many ways to defend our homes may be illegal, but

lawful options include various brands of door locks or wall safes. And, as citizens, we can influence social and government policies.

I'm going to help you make sensible security trade-offs by teaching you how to think about security. Much of what I'm going to say is in stark contrast to the things you hear on television and the things our politicians are telling us. I read the newspapers, too, and the things we're asked to accept continually incense me. I've watched the creation of a new cabinet-level Department of Homeland Security. I've seen budget expenditures for security reaching $33.7 billion in 2003, and even more in future years. We're being asked to pay a lot for security, and not just in dollars. I'd like to see us get our money's worth.

Security is both a feeling and a reality. We're secure when we feel protected from harm, free from dangers, and safe from attack. In this way, security is merely a state of mind. But there's the reality of security as well, a reality that has nothing do with how we feel. We're secure when we actually *are* protected. Although both are important, this book is more about the reality of security than the feeling. We need to feel in control and positive and not harried and fearful for security to have much of a positive effect on our daily lives; living in a state of constant fear, after all, would take away many of the benefits we want from real security. But it's nonetheless important to ground that feeling of security in the reality of security, and not merely in placebos.

In some ways, this is analogous to health. If you went to the doctor because you had a badly damaged leg, she wouldn't pretend that she could return your leg to its undamaged state if she couldn't. She would tell you the truth, describe your treatment options, and help you choose the one that's best for you. Ignoring reality is not an effective way to get healthier, or smarter, or safer, even though it might temporarily make you feel better.

• • • •

Security is not an isolated good, but just one component of a complicated transaction. It costs money, but it can also cost in intangibles: time, convenience, flexibility, or privacy. You will be able to intelligently assess these trade-offs. I won't tell you what you *want* to buy or which national security policies to support—these are personal decisions—but I will give you the tools you need to make those decisions for yourself. No security is foolproof, but neither is all security equal. There's cheap security and expensive security. There's unobtrusive security and security that forces us to change how we live. There's

security that respects our liberties and there's security that doesn't. There's security that really makes us safer and security that only lets us feel safer, with no reality behind it.

You face the same challenges with other choices. Your doctor can urge you to quit smoking, to exercise regularly, or to go on a low-cholesterol diet. But each of these actions requires trade-offs, and as a patient you may not choose to do the things your doctor recommends. You may not want to put in the time. You may be unwilling to make the trade-offs necessary to change your habits. You may not be able to afford the cost of treatment. You may be seduced by a guy selling weight-loss systems or herbal remedies on late-night TV.

A common path to bad security is knee-jerk reactions to the news of the day. Too much of the U.S. government's response post-9/11 is exactly that. We are told that we are in graver danger than ever, and that we must change our lives in drastic and inconvenient ways in order to be secure. We are told that we must sacrifice privacy and anonymity and accept restrictions on our actions. We are told that the police need new far-reaching investigative powers, that domestic spying capabilities need to be instituted, that our militaries must be brought to bear on countries that support terrorism, and that we must spy on each other. The security "doctors" are telling us to trust them, that all these changes are for our own good.

But the reality is that most of the changes we're being asked to endure won't result in good security. They're Band-Aids that ignore the real problems. Some of these changes may enhance our feeling of security, but would actually make us less safe. Our legislatures are not spending enough time examining the consequences of these so-called security measures. As you'll see in the next chapter, security is always a trade-off, and to ignore or deny those trade-offs is to risk losing basic freedoms and ways of life we now take for granted.

When you understand security and are able to make sensible trade-offs, you become actively involved in these security decisions and won't accept uncritically whatever is being offered to you. You may not be able to directly affect public policy, but you can decide whether to use the security provided or to do something else. You will be able to intelligently make your own trade-offs. And en masse, you can eventually change public policy.

• • • •

The world is a dangerous place, but it's also a good and decent place. People are good. People are kind. People are nice. Even in the worst neighborhoods, most people are safe. If Al Qaeda has 5,000 members, this is still only one in a million people worldwide, and if they were all in America, only one in 60,000. It's hard to find a terrorist, kidnapper, or bank robber, because there simply aren't that many in our society.

The point here is—and it's an important one to keep in mind—security exists to deal with the few bad apples, but if we allow those antisocial types to dictate social policy for everyone, we're making a mistake. Perfect security is impractical because the costs are simply too high; we would have to treat the whole world as a threatening place and all the people in it as evildoers, when in fact the real threats are not nearly so pervasive. We'd have to create an extremely oppressive regime. But freedom is security. Openness is security. If you want proof, look around you. The world's liberal democracies are the safest societies on the planet. Countries like the former Soviet Union, the former East Germany, Iraq, North Korea, and China tried to implement large-scale security systems across their entire populaces. Would anyone willingly trade the dangerous openness of the U.S. or most countries in Europe for the security of a police state or totalitarian government?

When you're scared, it's easy to lock the doors and head for the cellar. It's easy to demand that "something must be done" and that "those responsible must pay." It's easy to reach for the feeling of security and ignore its reality. But, remember, security catastrophes are extremely rare events. Making large changes in response to rare events often doesn't make sense, because these infrequent occurrences seldom have anything to do with day-to-day life. People shouldn't let their fears dominate their everyday life; there just aren't enough bad apples around.

Security is complicated and challenging. Easy answers won't help, because the easy answers are invariably the wrong ones. What you need is a new way to think.

• • • •

All security is, in some way, about prevention. But prevention of what, exactly? Security is about *preventing adverse consequences from the intentional and unwarranted actions of others*. What this definition basically means is that we want people to behave in a certain way—to pay for items at a store before walking out with them, to honor contracts they sign, to not shoot or bomb each other—and security is a way of ensur-

ing that they do so. Obviously, if people always did what they were supposed to do, there would be no need for security. But because not everyone does, security is critical to every aspect of society. The definition above tries to brings these issues into focus.

- Security is about prevention. A *security system* is the set of things put in place, or done, to prevent adverse consequences. Cars have antitheft security systems. The money in your wallet has a variety of anti-counterfeiting security systems. Airports and airplanes have many overlapping security systems. Some security systems, like financial audits, don't stop criminals but reduce or prevent the adverse consequences of their crimes. (This type of after-the-fact security system has a deterrence effect, which acts as a form of prevention.) Like any other system, security systems can be attacked, can have flaws, and can fail.
- Security concerns itself with *intentional* actions. This points to an important distinction: Protecting assets from unintentional actions is safety, not security. While it is common to talk about securing ourselves against accidents or from natural disasters, in this book I try to restrict the discussion to security from intentional actions. In some ways this is an arbitrary distinction, because safety and security are similar, and the things that protect from one also protect from the other. And, in fact, safety is often more important than security, since there are far more unintentional unwarranted actions in the world than intentional ones. I make the distinction for the purpose of limiting the scope of this book.
- These intentional actions are *unwarranted* from the point of view of the *defender*. Note that the unwarranted actions are not necessarily illegal.
- Security requires the concept of an *attacker* who performs these intentional and unwarranted actions. It's important to understand that this term is meant to be nonpejorative, value-neutral. Attackers may be on your side. Burglars are criminals, but police officers who attack a drug lord in his mountain hideout are the good guys. Sometimes the attacker isn't even human, as in the case of a tiger trying to pry open your Land Rover and eat you. The term *attacker* assumes nothing about the morality or the legality of the attack. It doesn't even imply malicious intent, although that certainly is often involved.

- Those intentional unwarranted actions are called *attacks*. An attack is a specific way to attempt to break the security of a system or a component of a system. It can refer to an abstraction—"You can successfully attack a house by breaking a window"—or it can refer to a specific incident—"On 7 September 1876, the Jesse James Gang attacked the First National Bank of Northfield in Northfield, Minnesota."
- The objects of attack are *assets*. Assets can be as small as a single diamond and as large as a nation's infrastructure.
- Security can also refer to the mechanisms used to provide the protection. In this book, the individual, discrete, and independent security components are called *countermeasures*. Countermeasures include door locks, guards, ID cards, and the metallic thread in banknotes that makes them more difficult to counterfeit. Walls, alarms, cryptography, pots of boiling oil you can pour on the heads of people invading your castle—these are all countermeasures. A security system consists of a series of countermeasures.

Unfortunately, many countermeasures are ineffective. Either they do not prevent adverse consequences from the intentional and unwarranted actions of people, or the trade-offs simply aren't worth it. Those who design and implement bad security don't seem to understand how security works or how to make security trade-offs. They spend too much money on the wrong kinds of security. They make the same mistakes over and over. And they're constantly surprised when things don't work out as they'd intended.

One problem is caused by an unwillingness on the part of the engineers, law enforcement agencies, and civic leaders involved in security to face the realities of security. They're unwilling to tell the public to accept that there are no easy answers and no free rides. They have to be seen as doing something, and often they are seduced by the promise of technology. They believe that because technology can solve a multitude of problems and improve our lives in countless ways, it can solve security problems in a similar manner. But it's not the same thing. Technology is generally an enabler, allowing people to do things. Security is the opposite: It tries to prevent something from happening, or prevent people from doing something, in the face of someone actively trying to defeat it. That's why technology doesn't work in security the way it does elsewhere, and why an overreliance on technology often leads to bad security, or even to the opposite of security.

The sad truth is that bad security can be worse than no security; that is, by trying and failing to make ourselves more secure, we make ourselves less secure. We spend time, money, and energy creating systems that can themselves be attacked easily and, in some cases, that don't even address the real threats. We make poor trade-offs, giving up much in exchange for very little security. We surround ourselves with security countermeasures that give us a feeling of security rather than the reality of security. We deceive ourselves by believing in security that doesn't work.

• • • •

Security is complex, but complex things can be broken down into smaller and simpler steps. Throughout this book, I use a five-step process to analyze and evaluate security systems, technologies, and practices. Each of these five steps contains a question that is intended to help you focus on a particular security system or security countermeasure. The questions may seem, at first, to be obvious, even trivial. But if you bear with me, and take them seriously, you will find they will help you determine which kinds of security make sense and which don't.

- *Step 1: What assets are you trying to protect?* This question might seem basic, but a surprising number of people never ask it. The question involves understanding the scope of the problem. For example, securing an airplane, an airport, commercial aviation, the transportation system, and a nation against terrorism are all different security problems, and require different solutions.
- *Step 2: What are the risks to these assets?* Here we consider the need for security. Answering it involves understanding what is being defended, what the consequences are if it is successfully attacked, who wants to attack it, how they might attack it, and why.
- *Step 3: How well does the security solution mitigate those risks?* Another seemingly obvious question, but one that is frequently ignored. If the security solution doesn't solve the problem, it's no good. This is not as simple as looking at the security solution and seeing how well it works. It involves looking at how the security solution interacts with everything around it, evaluating both its operation and its failures.
- *Step 4: What other risks does the security solution cause?* This question addresses what might be called the problem of unintended consequences. Security solutions have ripple effects, and most cause

new security problems. The trick is to understand the new problems and make sure they are smaller than the old ones.

- *Step 5: What costs and trade-offs does the security solution impose?* Every security system has costs and requires trade-offs. Most security costs money, sometimes substantial amounts; but other trade-offs may be more important, ranging from matters of convenience and comfort to issues involving basic freedoms like privacy. Understanding these trade-offs is essential.

These five steps don't lead to an answer, but rather provide the mechanism to evaluate a proposed answer. They lead to another question: Is the security solution worth it? In other words, is the benefit of mitigating the risks (Step 3) worth the additional risks (Step 4) plus the other trade-offs (Step 5)? It is not enough for a security measure to be effective. We don't have limitless resources or infinite patience. As individuals and a society, we need to do the things that make the most sense, that are the most effective use of our security dollar. But, as you'll see later in this book, subjective (and sometimes arbitrary) economic incentives make an enormous difference as to which security solutions are cost-effective and which ones aren't.

These five steps may seem obvious when stated in this abstract form, but applying them to real situations is hard work. Step 3, for example, requires you to understand the security solution and how well it actually works—not merely as described in the manufacturer's literature or as explained to you by a politician, but in real situations against real attackers. Step 5 requires you to understand the variety of trade-offs a security solution imposes, how it interacts with other aspects of your life, and what ancillary security solutions are required to make it work. The answers aren't always easy to come by. It's hard to quantify any of the steps, including the threat. Sometimes you won't have enough information, and you will be forced to make your best guess. Sometimes you'll be comparing apples and oranges. It can quickly become very complex and subjective.

Keep the steps in mind as you read the many examples in this book, and as you encounter and interact with the thousands of security systems that surround you every day, you'll start to notice the difference between good and bad security or security that could be designed better or require less onerous trade-offs. You'll begin to realize how ineffectual some common security systems are: how they solve the wrong problem or cause more problems than they solve. You'll start

making different security decisions: choosing more security in some instances and less security in others. You'll become more aware of the security trade-offs being imposed on you. And because security is all of a piece, the same knowledge will make you better able to choose a home alarm, and better equipped to participate in the national security policy debates.