behind the scenes

chapter 1

Security's Weakest Link

A company may have purchased the best security technologies that money can buy, trained their people so well that they lock up all their secrets before going home at night, and hired building guards from the best security firm in the business.

That company is still totally vulnerable.

Individuals may follow every best-security practice recommended by the experts, slavishly install every recommended security product, and be thoroughly vigilant about proper system configuration and applying security patches.

Those individuals are still completely vulnerable.

THE HUMAN FACTOR

Testifying before Congress not long ago, I explained that I could often get passwords and other pieces of sensitive information from companies by pretending to be someone else and *just asking for it*.

It's natural to yearn for a feeling of absolute safety, leading many people to settle for a false sense of security. Consider the responsible and loving homeowner who has a Medico, a tumbler lock known as being pickproof, installed in his front door to protect his wife, his children, and his home. He's now comfortable that he has made his family much safer against intruders. But what about the intruder who breaks a window, or cracks the code to the garage door opener? How about installing a robust security system? Better, but still no guarantee. Expensive locks or no, the homeowner remains vulnerable.

Why? Because the *human* factor is truly security's weakest link.

Security is too often merely an illusion, an illusion sometimes made even worse when gullibility, naïveté, or ignorance come into play. The world's most respected scientist of the twentieth century, Albert Einstein, is quoted as saying, "Only two things are infinite, the universe and human stupidity, and I'm not sure about the former." In the end, social engineering attacks can succeed when people are stupid or, more commonly, simply ignorant about good security practices. With the same attitude as our security-conscious homeowner, many information technology (IT) professionals hold to the misconception that they've made their companies largely immune to attack because they've deployed standard security products—firewalls, intrusion detection systems, or stronger authentication devices such as time-based tokens or biometric smart cards. Anyone who thinks that security products alone offer true security is settling for the *illusion* of security. It's a case of living in a world of fantasy: They will inevitably, later if not sooner, suffer a security incident.

As noted security consultant Bruce Schneier puts it, "Security is not a product, it's a process." Moreover, security is not a technology problem—it's a people and management problem.

As developers invent continually better security technologies, making it increasingly difficult to exploit technical vulnerabilities, attackers will turn more and more to exploiting the human element. Cracking the human firewall is often easy, requires no investment beyond the cost of a phone call, and involves minimal risk.

A CLASSIC CASE OF DECEPTION

What's the greatest threat to the security of your business assets? That's easy: the social engineer—an unscrupulous magician who has you watching his left hand while with his right he steals your secrets. This character is often so friendly, glib, and obliging that you're grateful for having encountered him.

Take a look at an example of social engineering. Not many people today still remember the young man named Stanley Mark Rifkin and his little adventure with the now defunct Security Pacific National Bank in Los Angeles. Accounts of his escapade vary, and Rifkin (like me) has never told his own story, so the following is based on published reports.

Code Breaking

One day in 1978, Rifkin moseyed over to Security Pacific's authorized-personnel-only wire-transfer room, where the staff sent and received transfers totaling several billion dollars every day.

He was working for a company under contract to develop a backup system for the wire room's data in case their main computer ever went down. That role gave him access to the transfer procedures, including how bank officials arranged for a transfer to be sent. He had learned that bank officers who were authorized to order wire transfers would be given a closely guarded daily code each morning to use when calling the wire room.

In the wire room the clerks saved themselves the trouble of trying to memorize each day's code: They wrote down the code on a slip of paper and posted it where they could see it easily. This particular November day Rifkin had a specific reason for his visit. He wanted to get a glance at that paper.

Arriving in the wire room, he took some notes on operating procedures, supposedly to make sure the backup system would mesh properly with the regular systems. Meanwhile, he surreptitiously read the security code from the posted slip of paper, and memorized it. A few minutes later he walked out. As he said afterward, he felt as if he had just won the lottery.

There's This Swiss Bank Account . . .

Leaving the room at about 3 o'clock in the afternoon, he headed straight for the pay phone in the building's marble lobby, where he deposited a coin and dialed into the wire-transfer room. He then changed hats, transforming himself from Stanley Rifkin, bank consultant, into Mike Hansen, a member of the bank's International Department.

According to one source, the conversation went something like this:

"Hi, this is Mike Hansen in International," he said to the young woman who answered the phone.

She asked for the office number. That was standard procedure, and he was prepared: "286," he said.

The girl then asked, "Okay, what's the code?"

Rifkin has said that his adrenaline-powered heartbeat "picked up its pace" at this point. He responded smoothly, "4789." Then he went on to give instructions for wiring "Ten million, two-hundred thousand dollars exactly" to the Irving Trust Company in New York, for credit of the Wozchod Handels Bank of Zurich, Switzerland, where he had already established an account.

The girl then said, "Okay, I got that. And now I need the interoffice settlement number."

Rifkin broke out in a sweat; this was a question he hadn't anticipated, something that had slipped through the cracks in his research. But he

managed to stay in character, acted as if everything was fine, and on the spot answered without missing a beat, "Let me check; I'll call you right back." He changed hats once again to call another department at the bank, this time claiming to be an employee in the wire-transfer room. He obtained the settlement number and called the girl back.

She took the number and said, "Thanks." (Under the circumstances, her thanking him has to be considered highly ironic.)

Achieving Closure

A few days later Rifkin flew to Switzerland, picked up his cash, and handed over $8 million to a Russian agency for a pile of diamonds. He flew back, passing through U.S. Customs with the stones hidden in a money belt. He had pulled off the biggest bank heist in history—and done it without using a gun, even without a computer. Oddly, his caper eventually made it into the pages of the *Guinness Book of World Records* in the category of "biggest computer fraud."

Stanley Rifkin had used the art of deception—the skills and techniques that are today called social engineering. Thorough planning and a good gift of gab is all it really took.

And that's what this book is about—the techniques of social engineering (at which yours truly is proficient) and how to defend against their being used at your company.

THE NATURE OF THE THREAT

The Rifkin story makes perfectly clear how misleading our sense of security can be. Incidents like this—okay, maybe not $10 million heists, but harmful incidents nonetheless—are happening *every day.* You may be losing money right now, or somebody may be stealing new product plans, and you don't even know it. If it hasn't already happened to your company, it's not a question of *if* it will happen, but *when*.

A Growing Concern

The Computer Security Institute, in its 2001 survey of computer crime, reported that 85 percent of responding organizations had detected computer security breaches in the preceding twelve months. That's an astounding number: Only fifteen out of every hundred organizations responding were able to say that they had not had a security breach during the year. Equally astounding was the number of organizations that reported that they had experienced financial losses due to computer

breaches: 64 percent. Well over half the organizations had suffered financially. *In a single year*.

My own experiences lead me to believe that the numbers in reports like this are somewhat inflated. I'm suspicious of the agenda of the people conducting the survey. But that's not to say that the damage isn't extensive; it is. Those who fail to plan for a security incident are planning for failure.

Commercial security products deployed in most companies are mainly aimed at providing protection against the amateur computer intruder, like the youngsters known as script kiddies. In fact, these wannabe hackers with downloaded software are mostly just a nuisance. The greater losses, the real threats, come from sophisticated attackers with well-defined targets who are motivated by financial gain. These people focus on one target at a time rather than, like the amateurs, trying to infiltrate as many systems as possible. While amateur computer intruders simply go for quantity, the professionals target information of quality and value.

Technologies like authentication devices (for proving identity), access control (for managing access to files and system resources), and intrusion detection systems (the electronic equivalent of burglar alarms) are necessary to a corporate security program. Yet it's typical today for a company to spend more money on coffee than on deploying countermeasures to protect the organization against security attacks.

Just as the criminal mind cannot resist temptation, the hacker mind is driven to find ways around powerful security technology safeguards. And in many cases, they do that by targeting the people who use the technology.

Deceptive Practices

There's a popular saying that a secure computer is one that's turned off. Clever, but false: The *pretexter* simply talks someone into going into the office and turning that computer on. An adversary who wants your information can obtain it, usually in any one of several different ways. It's just a matter of time, patience, personality, and persistence. That's where the art of deception comes in.

To defeat security measures, an attacker, intruder, or social engineer must find a way to deceive a trusted user into revealing information, or trick an unsuspecting mark into providing him with access. When trusted employees are deceived, influenced, or manipulated into revealing sensitive information, or performing actions that create a security hole for the attacker to slip through, no technology in the world can protect a business. Just as cryptanalysts are sometimes able to reveal the plain text of a coded message by finding a weakness that lets them bypass the encryption

technology, social engineers use deception practiced on your employees to bypass security technology.

ABUSE OF TRUST

In most cases, successful social engineers have strong people skills. They're charming, polite, and easy to like—social traits needed for establishing rapid rapport and trust. An experienced social engineer is able to gain access to virtually any targeted information by using the strategies and tactics of his craft.

Savvy technologists have painstakingly developed information-security solutions to minimize the risks connected with the use of computers, yet left unaddressed the most significant vulnerability, the human factor. Despite our intellect, we humans—you, me, and everyone else—remain the most severe threat to each other's security.

Our National Character

We're not mindful of the threat, especially in the Western world. In the United States most of all, we're not trained to be suspicious of each other. We are taught to "love thy neighbor" and have trust and faith in each other. Consider how difficult it is for neighborhood watch organizations to get people to lock their homes and cars. This sort of vulnerability is obvious, and yet it seems to be ignored by many who prefer to live in a dream world—until they get burned.

We know that all people are not kind and honest, but too often we live as if they were. This lovely innocence has been the fabric of the lives of Americans and it's painful to give it up. As a nation we have built into our concept of freedom that the best places to live are those where locks and keys are the least necessary.

Most people go on the assumption that they will not be deceived by others, based upon a belief that the probability of being deceived is very low; the attacker, understanding this common belief, makes his request sound so reasonable that it raises no suspicion, all the while exploiting the victim's trust.

Organizational Innocence

That innocence that is part of our national character was evident back when computers were first being connected remotely. Recall that the ARPANet (the Defense Department's Advanced Research Projects Agency

Network), the predecessor of the Internet, was designed as a way of sharing research information between government, research, and educational institutions. The goal was information freedom, as well as technological advancement. Many educational institutions therefore set up early computer systems with little or no security. One noted software libertarian, Richard Stallman, even refused to protect his account with a password.

But with the Internet being used for electronic commerce, the dangers of weak security in our wired world have changed dramatically. Deploying more technology is not going to solve the human security problem.

Just look at our airports today. Security has become paramount, yet we're alarmed by media reports of travelers who have been able to circumvent security and carry potential weapons past checkpoints. How is this possible during a time when our airports are on such a state of alert? Are the metal detectors failing? No. The problem isn't the machines. The problem is the human factor: The people manning the machines. Airport officials can marshal the National Guard and install metal detectors and facial recognition systems, but educating the frontline security staff on how to properly screen passengers is much more likely to help.

The same problem exists within government, business, and educational institutions throughout the world. Despite the efforts of security professionals, information everywhere remains vulnerable and will continue to be seen as a ripe target by attackers with social engineering skills, until the weakest link in the security chain, the human link, has been strengthened.

Now more than ever we must learn to stop wishful thinking and become more aware of the techniques that are being used by those who attempt to attack the confidentiality, integrity, and availability of our computer systems and networks. We've come to accept the need for defensive driving; it's time to accept and learn the practice of defensive computing.

The threat of a break-in that violates your privacy, your mind, or your company's information systems may not seem real until it happens. To avoid such a costly dose of reality, we all need to become aware, educated, vigilant, and aggressively protective of our information assets, our own personal information, and our nation's critical infrastructures. And we must implement those precautions today.

TERRORISTS AND DECEPTION

Of course, deception isn't an exclusive tool of the social engineer. Physical terrorism makes the biggest news, and we have come to realize as never

before that the world is a dangerous place. Civilization is, after all, just a thin veneer.

The attacks on New York and Washington, D.C., in September 2001 infused sadness and fear into the hearts of every one of us—not just Americans, but well-meaning people of all nations. We're now alerted to the fact that there are obsessive terrorists located around the globe, well-trained and waiting to launch further attacks against us.

The recently intensified effort by our government has increased the levels of our security consciousness. We need to stay alert, on guard against all forms of terrorism. We need to understand how terrorists treacherously create false identities, assume roles as students and neighbors, and melt into the crowd. They mask their true beliefs while they plot against us—practicing tricks of deception similar to those you will read about in these pages.

And while, to the best of my knowledge, terrorists have not yet used social engineering ruses to infiltrate corporations, water-treatment plants, electrical generation facilities, or other vital components of our national infrastructure, the potential is there. It's just too easy. The security awareness and security policies that I hope will be put into place and enforced by corporate senior management because of this book will come none too soon.

ABOUT THIS BOOK

Corporate security is a question of balance. Too little security leaves your company vulnerable, but an overemphasis on security gets in the way of attending to business, inhibiting the company's growth and prosperity. The challenge is to achieve a balance between security and productivity.

Other books on corporate security focus on hardware and software technology, and do not adequately cover the most serious threat of all: human deception. The purpose of this book, in contrast, is to help you understand how you, your coworkers, and others in your company are being manipulated, and the barriers you can erect to stop being victims. The book focuses mainly on the non-technical methods that hostile intruders use to steal information, compromise the integrity of information that is believed to be safe but isn't, or destroy company work product.

My task is made more difficult by a simple truth: Every reader will have been manipulated by the grand experts of all time in social engineering—their parents. They found ways to get you—"for your own good"—to do

what they thought best. Parents become great storytellers in the same way that social engineers skillfully develop very plausible stories, reasons, and justifications for achieving their goals. Yes, we were all molded by our parents: benevolent (and sometimes not so benevolent) social engineers.

Conditioned by that training, we have become vulnerable to manipulation. We would live a difficult life if we had to be always on our guard, mistrustful of others, concerned that we might become the dupe of someone trying to take advantage of us. In a perfect world we would implicitly trust others, confident that the people we encounter are going to be honest and trustworthy. But we do not live in a perfect world, and so we have to exercise a standard of vigilance to repel the deceptive efforts of our adversaries.

The main portions of this book, Parts 2 and 3, are made up of stories that show you social engineers in action. In these sections you'll read about:

- What phone phreaks discovered years ago: A slick method for getting an unlisted phone number from the telephone company.
- Several different methods used by attackers to convince even alert, suspicious employees to reveal their computer usernames and passwords.
- How an Operations Center manager cooperated in allowing an attacker to steal his company's most secret product information.
- The methods of an attacker who deceived a lady into downloading software that spies on every keystroke she makes and emails the details to him.
- How private investigators get information about your company, and about you personally, that I can practically guarantee will send a chill up your spine.

You might think as you read some of the stories in Parts 2 and 3 that they're not possible, that no one could really succeed in getting away with the lies, dirty tricks, and schemes described in these pages. The reality is that in every case, these stories depict events that can and do happen; many of them are happening every day somewhere on the planet, maybe even to your business as you read this book.

The material in this book will be a real eye-opener when it comes to protecting your business, but also personally deflecting the advances of a social engineer to protect the integrity of information in your private life.

In Part 4 of this book I switch gears. My goal here is to help you create the necessary business policies and awareness training to minimize the chances of your employees ever being duped by a social engineer. Understanding the strategies, methods, and tactics of the social engineer will help prepare you to deploy reasonable controls to safeguard your IT assets, without undermining your company's productivity.

In short, I've written this book to raise your awareness about the serious threat posed by social engineering, and to help you make sure that your company and its employees are less likely to be exploited in this way.

Or perhaps I should say, far less likely to be exploited *ever again*.