

Chapter 1

Are You the Weakest Link?

As you read this sentence, your friends and co-workers will make mistakes that cost your employers and the economy millions of dollars. In the next sixty seconds:

- Five people will become victims of credit card fraud or identity theft, costing businesses an average loss of \$4,000.00 per incident. One of these five people will never recover their damaged credit.
- Roughly 300 credit card numbers will be stolen from corporations where we work. Many of these will be used to steal money to fund organized crime or terrorism.
- Employees at 9 out of 10 companies will have recently sent private information such as a credit card, social security number or both out into the internet for easy capture by thieves.
- Thousands of our home personal computers will send out millions of spam messages to our employers and other companies around the world without us even knowing it.

Notice I said “co-workers.” Certainly this isn’t you. Or is it? Can you even be sure? The simple truth is that information systems have become so complex and so interconnected that most of us don’t have a good idea of what, how and where information is

stored. Most of us are conscientious employees, doing our jobs to the best of our ability. We try to follow the correct procedures that our companies have told us about. While this may be true, the reality is that many of us are unwitting accomplices in a world-wide crime ring that is growing at an alarming rate. Most of us have no idea that we are putting ourselves, our employers, our co-workers and our loved-ones at risk. If we *are* aware, we don't really know what to do about it.

This book is designed with three simple goals:

1. To make you aware, using real-world examples, how you can easily become part of information breaches and crimes.
2. To motivate you to become part of the solution rather than part of the problem.
3. To give you some simple rules that will help protect yourself and your organization from problems that may cost thousands or millions of dollars.

The first step to understanding your role in information security is to understand your personal network.

The Network Effect

We are all part of a network of connected people. Most of us are part of many networks. For example, your immediate family, your church, your community organizations, and your place of employment are all networks. And people become connected to their networks through shared information. Think about it. What do you have in common with the various people you are connected to in these networks? In many cases, it is the information, in the form of data, rules, beliefs, stories and traditions that help create the

shared experience of a network. While this shared experience, let's call it "connectedness" provides much value, it also creates risk. Because of this shared experience, many of us implicitly trust other people in our network. Criminals who are aware of this understand that you can exploit a network once you gain trusted access to a single part. There is a fundamental law of information security that goes like this:

A network is only as secure as the weakest point.

There are many examples that bear out this truth. One of the most devastating was the New York City terrorist attacks on 9/11/2001.

It is important to remember that the terrorist attacks on 9/11 were not merely a single catastrophic event – but a culmination of a large number of security lapses strung together. That is how most attacks occur, in cyberspace or otherwise. The person who is going to attack a target must be aware of a vulnerability – or weakness – in the target, and get in position to exploit that weakness. Usually this is done through a series of smaller steps that enable the final attack.

For a computer hacker, he or she must first steal a username and then crack a password. This can be done by making a phone call, or "dumpster diving" for important information that was carelessly thrown away. Once he is in, there needs to be a system weakness that can be exploited, such as files or applications that are not protected. And once a weakness is exploited, the good attacker needs to be knowledgeable enough to cover his tracks.

In the terrorist attacks, there were forged passports and driver's licenses, intelligence lapses, poor communications, and passengers that bought one-way airline tickets with cash. Independently, these were not necessarily threatening events, but together they became disastrous. So before this very large physical attack, there were

many small information attacks that enabled it. Think about how the future might have been changed if just one knowledgeable person – at the passport photo center, at the flight school, at the car rental agency, or at the ticket counter – had the knowledge to connect the relevant pieces of information and the confidence to step forward.

While the idea of fighting terrorism is pretty remote for most of us, the concept of connections translates to each and every one of us. We are part of many networks, and each day we touch information that is critical to the overall security of our network. If we are not aware of what can happen, we are likely to become unwitting accomplices in a security breach that might harm others in our network.

I believe this is the obligation that faces all of us today. Since we are all part of many trusted networks, by learning to protect ourselves we make each of our networks more secure.

When bad things happen to good companies

If you pay attention to the news, you have heard or read stories about major information security breaches occurring at a frightening rate. Consider this:

In 2005 alone, over 130 reported data privacy breaches exposed the personal information of over 50 million people.

Just in case you missed them, here are a few of the most recent high-profile cases in the news.

- In early 2005, DSW Shoe warehouse had approximately 1.2 million credit cards stolen from databases in various stores. In addition, some 100,000 checking accounts and matching driver's licenses were also stolen.
- In early 2005, ChoicePoint Inc. announced that criminals posing as legitimate businesses had stolen personal information for over 145,000 consumers. ChoicePoint reported that as of June 2005 the information stolen had been used in around 750 identity-theft scams.
- In June 2005, CitiFinancial reported that they lost a backup tape with financial information on 3.9 million customers.
- Later in the same month, CardSystems Solutions, a company who processes credit cards for major card companies, reported that over 40 million credit cards could have been stolen. That is nearly one out of every 6 people in the United States.
- In January 2006, resort owner Kerzner International announced that a database security breach exposed the personal information of over 55,000 resort customers.
- In June 2006, an employee laptop was stolen which exposed the personal information of over 26 million military personnel from the Veterans Administration.

Chances are, by the time you read this there will be others. In some cases, these companies will get fined hundreds of thousands or even millions of dollars. For some, their stock price will sink temporarily or permanently, removing millions in shareholder value. Some may go out of business entirely.

So what is wrong here? Are these companies, just like the ones you and I work for, completely lax in their information security? Do they blatantly disregard their customers' need for privacy and their employees' need for security? In most cases, no. In some cases, yes. In fact, many of the corporations that have issues with information security are otherwise extremely well run companies. Chances are, you work for one. So what IS going on?

Three reasons why corporate security often fails

While certainly some companies might be severely lacking in their information security programs, I believe there are simpler and less-devious reasons. Two of them you can't do anything about, and the last one you can.

1. Most corporations are in business to make money, not protect information.

If you think about it, the primary reason that most businesses are in business is to make money. In order to make money, they need to process information. For many businesses protecting this information is, at best, an afterthought. For some business sectors, such as banks and healthcare, the Federal government had to step in and pass legislation requiring companies to protect information. Dozens of companies have received fines or sanctions costing them millions of dollars. In fact, over 100 U.S. and international laws have been passed with the goal of protecting information. And still the problems continue.

2. When people and information mix, there are going to be problems.

People make mistakes. It is our very nature. Most of us work in environments saturated with information. In trying to process and digest all of this information, we use computers and other information systems that we are remotely familiar with. Computers rarely make mistakes all by themselves. It is always a person, interacting with the information in some unexpected way that makes the information vulnerable, leading to a possible information breach.

3. Information security is too complicated to be managed by a small group of people. The employees must be on the team.

In the past, the protection of information could be managed by a small group of people. The idea that one smaller group can protect a large community has been the security model for thousands of years. However, as we will see in the next chapter, in a modern corporation there is too much data, in too many different formats and in too many different places. In short, the average corporate citizen in today's environment has a lot of sensitive information at their fingertips and access to powerful technology that is easy to misuse. One of the goals of this book is to convince you of this next fundamental law of information security:

The problem of information security, and the resulting costs to our economy and national security, is a hopeless battle unless you get on the team.

An overall lack of understanding

At this point you might be tempted to throw up your hands and say, “those are the big, bad companies behaving in big, bad ways.” It’s easy to blame corporations. But consider this: In each and every case of a data breach there are employees who manage this data and the systems that process the data.

So while our companies’ might not be doing a good job or protecting information, as individuals we are doing worse. In fact, a quick look at the data shows that as individuals, we are not very savvy about information security. Consider some of these statistics:

- In their annual National Crime Victimization Survey, the Department of Justice (DOJ) reported that in 2004 alone over 3.2 million people had become victims of identity theft. In many cases, the individuals are tricked into giving out their personal information to thieves.
- According to the Department of Justice, identity theft cost US consumers an estimated \$6.4 billion in 2005 and business as much as \$100 billion.
- A study by the Messaging Anti-Abuse Working Group estimates that 47 million personal computers are infected with “spyware” that may allow remote control by criminals and can send out millions of spam messages.

If you are like most people, you might read the headlines and either (1) not care, or (2) not even be aware that the problem was a failure of information security. If you *do* care, you might not be sure of what you can do about it personally. Unless it is our credit card that was lost or stolen, it is difficult to see how these problems affect us personally.

Some of you reading this might be thinking: Don't people know about computer viruses and hackers by now? The answer is yes, some people are aware of information security threats – but they generally have no idea what to do about them. To further the problem, criminals are getting more sophisticated and more organized, refining their attacks faster than we can learn about them.

Real World: According to a survey by Bentley College, 66% of users employed full or part-time have received no internet security training.

A 2005 study of American internet users by Bentley College and Symantec Corporation revealed some clues. The Bentley survey found that a large percentage of the public lacks knowledge about several Internet security issues:

- 90 percent say they have installed antivirus software, but 10 percent never or rarely update their antivirus software
- 75% of people are concerned about cyber-crime, but only 15% actually perform basic functions, like virus updates, to protect themselves
- 40 percent are not knowledgeable about spyware – software that send information secretly from your computer to others
- 49 percent are not knowledgeable about security flaws in Internet browsers
- 44 percent are not knowledgeable about the ability of hackers to hijack home computers and use them to send spam

Many people assume that even if they are lax about security on their home computers, that they will be protected at work. One growing problem is that many of us are connecting to the corporate network from home. By the year 2007, nearly 60 million people will be working remotely. As more people work remotely, the threat of

information security breaches infecting home PC's that then connect to the corporation is considerable.

Another problem is that many of our infected home computers can launch attacks against corporations through the internet. Computers infected with malicious software called spyware, can be remotely controlled by criminals to send keystrokes, important files or SPAM email messages. A collection of these infected computers working together is called a "botnet" and can wreak havoc due to the large number of computers operating at once.

Real World: According to a 2006 report by email security firm Sophos, over 50% of SPAM is sent by remotely controlled computers infected with spyware.

For example, in November 2005 FBI agents arrested Jeanson James Ancheta for spreading a malicious software program that allowed him to use over 400,000 computers. This spyware was routinely sending keystroke logs – basically a recording of what you type into the computer – to central collection points used for identity theft. If you realize that these same home computers are being used to connect back to a corporation, you can see how suddenly corporate data can make it out into the public internet, even without us knowing it.

Another problem is that most of us bring this lack of knowledge to work with us, allowing our corporate computers to become as vulnerable as the ones at home. Some recent studies even suggest the people are more lax about security at work than they are at home, assuming that the Information Technology (IT) department is taking care of them.

Real World: A recent survey of 1200 users in the U.S., Japan and Germany by internet security firm TrendMicro showed that most computer users are more lax about information security at work than they are at home.

There are two important points to take away from this discussion:

1. That information security breaches and computer crime are much bigger than you can imagine.
2. That you are much more likely to be part of the problem than you think.

For years, information security professionals, IT pundits and researchers have known what you might not: that people are the weakest link in security. That's right; YOU are the weakest link.

The Likely Point of Attack

Now you know what computer hackers and criminals have known for years: that humans are the weakest link in the security chain. And a good attacker always knows to go for the weakest link first. The chances are good that your employer has adopted lots of expensive technology to keep your organization secure, including "firewalls" and anti-virus software. However, as technology gets more sophisticated, it also gets harder to use and manage; it further increases the likelihood that a human mistake will create vulnerability. Kevin Mitnick, the notorious reformed hacker, author and computer security consultant sums it up in his book, *The Art of Deception*:

"As developers create continually better security technologies [...] hackers will turn more and more to the human element. Cracking the

human firewall is often easy, involves no more than the cost of a phone call, and involves minimal risk."

So the fact that you are the weakest link makes you even more vulnerable to an attack that will cost you or your company harm. It's a vicious cycle – unless you decide to do something about it.

You are the solution

Hopefully these stories serve to illustrate this important point: Individuals must become knowledgeable in the ways to protect information. If they do not, we are destined for a never ending war against cybercrime that will always be lost, one small battle at a time.

The good news is that since people are a critical part of this problem, YOU can become a crucial part of the solution. That is what this book is all about. Because you are part of many networks, making yourself more secure makes all of your networks more secure.

Chapter Summary

1. Information security breaches that put us and our employers at risk are increasing at an alarming rate.
2. We are all part of many networks, and networks are only as secure as the weakest link
3. In general, we are all fairly weak links due to the complexity of computer information systems and our lack of knowledge about how information is used.
4. Information security weaknesses at home can easily cause problems at work.
5. Because we are the weakest links, we are the most likely points of attack for computer criminals.
6. There is a way out.