CHAPTER 1

What Is Information Security?

Information security does not guarantee the safety of your organization or your information or your computer systems. Information security cannot, in and of itself, provide protection for your information. That being said, information security is also not a black art. There is no sorcery to implementing proper information security and the concepts that are included in information security are not rocket science.

In many ways, information security is a mindset. It is a mindset of examining the threats and vulnerabilities of your organization and managing them appropriately. Unfortunately, the history of information security is full of "silver bullets" that did nothing more than side-track organizations from proper risk management. Some product vendors assisted in this by claiming that their product was the solution to the security problem.

This chapter (and this book) will attempt to identify the myths about information security and show a more appropriate management strategy for organizations to follow.

DEFINING INFORMATION SECURITY

According to Merriam-Webster's online dictionary (**www.m-w.com**), information is defined as:

> *Knowledge obtained from investigation, study, or instruction, intelligence, news, facts, data, a signal or character (as in a communication system or computer) representing data, something (as a message, experimental data, or a picture) which justifies change in a construct (as a plan or theory) that represents physical or mental experience or another construct*

And security is defined as:

> *Freedom from danger, safety; freedom from fear or anxiety*

If we put these two definitions together we can come up with a definition of information security:

> *Measures adopted to prevent the unauthorized use, misuse, modification, or denial of use of knowledge, facts, data, or capabilities*

That definition encompasses quite a lot. It talks about all measures, whatever they may be, to prevent bad things from happening to knowledge, facts, data, or capabilities. We are also not limited to the form of the information. It might be knowledge or it might be capabilities.

However, this definition of information security does not guarantee protection. Information security cannot guarantee protection. We could build the biggest fortress in the world and someone could just come up with a bigger battering ram.

Information security is the name given to the preventative steps we take to guard our information and our capabilities. We guard these things against threats, and we guard them from the exploitation of a vulnerability.

BRIEF HISTORY OF SECURITY

How we handle the security of information and other assets has evolved over time as our society and technology have evolved. Understanding this evolution is important to understanding how we need to approach security today (hence the reason I am devoting some space to the history of security). The following sections follow security in a rough chronological order. If we learn from history, we are much less likely to repeat the mistakes of those who came before us.

Physical Security

Early in history, all assets were physical. Important information was also physical as it was carved into stone and later written on paper. (Actually, most historical leaders did not place sensitive/critical information in any permanent form, which is why there are very few records of alchemy. They also did not discuss it with anyone except their chosen disciples—knowledge was and is power. Maybe this was the best security. Sun Tzu said "A secret that is known by more than one is no longer a secret.") To protect these assets, physical security, such as walls, moats, and guards, was used.

If the information was transmitted, it usually went by messenger and usually with a guard. The danger was purely physical. There was no way to get at the information without physically grasping it. In most cases, the asset (money or written information) was stolen. The original owner of the asset was deprived of it.

Communications Security

Unfortunately, physical security had a flaw. If a message was captured in transit, the information in the message could be learned by an enemy. As far back as Julius Caesar, this flaw was identified. The solution was communications security. Julius Caesar created the Caesar cipher (see Chapter 12 for more information on this and other encryption systems). This cipher allowed him to send messages that could not be read if they were intercepted.

This concept continued into World War II. Germany used a machine called Enigma (see Figure 1-1) to encrypt messages sent to military units. The Germans considered Enigma to be unbreakable; if it had been used properly, it certainly would have been very difficult. As it was, some operator mistakes were made and the Allies were able to read some messages (after a considerable amount of resources were brought to bear on the problem).

Military communications also used code words for units and places in their messages. Japan used code words for their objectives during the war and that made true understanding of their messages difficult even though the United States had broken their code. During the lead-up to the Battle of Midway, American code breakers tried to identify the target referenced only as "AF" in Japanese messages. They finally had Midway send a message in the clear regarding a water shortage. The Japanese intercepted the message and sent a coded message noting that "AF" was short of water. Since the Americans were reading the Japanese messages, they were able to learn that "AF" was in fact Midway.

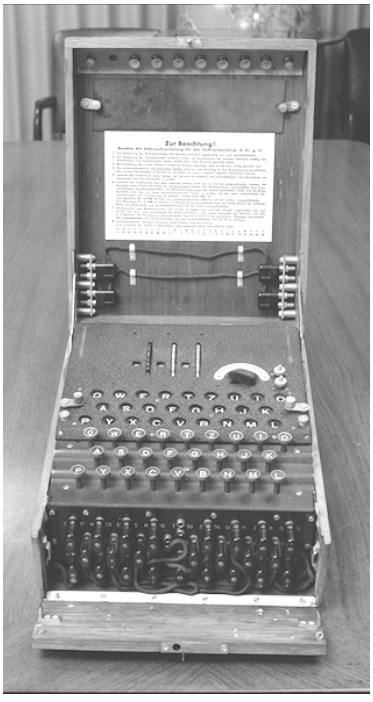

Figure 1-1. The Enigma machine

Messages were not the only type of traffic that was encoded. To guard against the enemy listening to voice messages, American military units used Navaho Code Talkers. The Navaho spoke their native language to transmit messages; if the enemy was listening to the radio traffic, they would not be able to understand the messages.

After World War II, the Soviet Union used one-time pads to protect information transmitted by spies. The one-time pads were literally pads of paper with random numbers on each page. Each page was used for one message and only one message. This encryption scheme is unbreakable if used properly, but the Soviet Union made the mistake of not using it properly (they reused the one-time pads) and thus some of the messages can be decrypted.

Emissions Security

Aside from mistakes in the use of encryption systems, good encryption is hard to break. Therefore, attempts were made to find other ways to capture information that was being transmitted in an encrypted form. In the 1950s, it was learned that access to messages could be achieved by looking at the electronic signals coming over phone lines (see Figure 1-2).

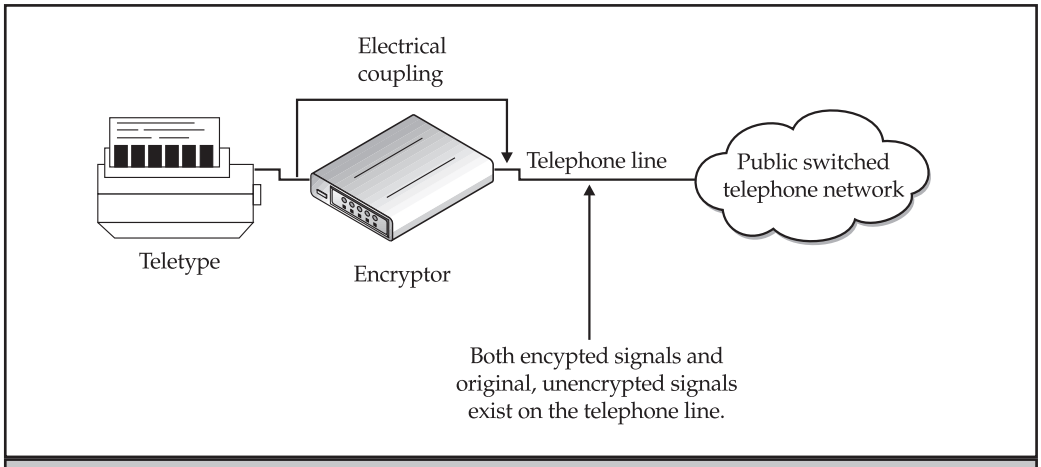

Figure 1-2. Electronic signals bypass encryption

All electronic systems give off electronic emissions. This includes the teletypes and the encryptors being used to send encrypted messages. The encryptor would take in the message, encrypt it, and send it out over a telephone line. It was found that electric signals representing the original message were also found on the telephone line. This meant that the messages could be recovered with some good equipment.

This problem caused the United States to create a program called TEMPEST. The TEMPEST program created electrical emissions standards for computer systems used in very sensitive environments. The goal was to reduce emissions that could be used to gather information.

Computer Security

Communications and emissions security were sufficient when messages were sent by teletype. Then computers came on the scene and most of the information assets of organizations migrated on to them in an electronic format. Over time, computers became easier to use and more people got access to them with interactive sessions. The information on the systems became accessible to anyone who had access to the system.

In the early 1970s, David Bell and Leonard La Padula developed a model for secure computer operations. This model was based on the government concept of various levels of classified information (unclassified, confidential, secret, and top secret) and various levels of clearances. Thus, if a person (a subject) had a clearance level that dominated (was higher than) the classification level of a file (an object), that person could access the file. If the person's clearance level was lower than the file's classification, access would be denied.

This concept of modeling eventually lead to United States Department of Defense Standard 5200.28, The Trusted Computing System Evaluation Criteria (TCSEC, also

known as the Orange Book) in 1983. The Orange Book defines computer systems according to the following scale:

D	Minimal Protection or Unrated
C1	Discretionary Security Protection
C2	Controlled Access Protection
B1	Labeled Security Protection
B2	Structured Protection
B3	Security Domains
A1	Verified Design

For each division, the Orange Book defined functional requirements as well as assurance requirements. Thus, in order for a system to meet the qualifications for a particular level of certification it had to meet the functional and the assurance requirements.

The assurance requirements for the more secure certifications took significant periods of time and cost the vendor a lot of money. This resulted in few systems being certified above C2 (in fact, only one system was ever certified A1, the Honeywell SCOMP) and the systems that were certified were obsolete by the time they completed the process.

Other criteria attempted to decouple functionality from assurance. These efforts included the German Green Book in 1989, the Canadian Criteria in 1990, the Information Technology Security Evaluation Criteria (ITSEC) in 1991, and the Federal Criteria in 1992. Each of these efforts attempted to find a method of certifying computer systems for security. The ITSEC and the Federal Criteria went so far as to leave functionality virtually undefined. The concept was that common application environments would develop their own profiles for security functionality and assurance levels. The profiles would then be used by some authority to certify the compliance of computer systems.

In the end, computer system technology moved too fast for certification programs. New versions of operating systems and hardware were being developed and marketed before an older system could be certified.

Network Security

One other problem related to the computer security evaluation criteria was the lack of a network understanding. When computers are networked together, new security issues arise and old issues arise in different ways. For example, we have communications but we have it over local area networks instead of wide area networks. We also have higher speeds and many connections to a common medium. Dedicated encryptors may not be the answer any more. We also have emissions from copper wire running throughout a room or building. And lastly, we have user access from many different systems without the central control of a single computer system.

The Orange Book did not address the issue of networked computers. In fact, network access could invalidate an Orange Book certification. The answer to this was the Trusted

Network Interpretation of the TCSEC (TNI, or the Red Book) in 1987. The Red Book took all of the requirements of the Orange Book and attempted to address a networked environment of computers. Unfortunately, it too linked functionality with assurance. Few systems were ever evaluated under the TNI and none achieved commercial success.

Information Security

So where does this history lead us? It would appear that none of the solutions by themselves solved all of the security problems. In fact, good security actually is a mix of all of these solutions (see Figure 1-3). Good physical security is necessary to protect physical assets like paper records and systems. Communication security (COMSEC) is necessary to protect information in transit. Emission security (EMSEC) is needed when the enemy has significant resources to read the electronic emissions from our computer systems. Computer security (COMPUSEC) is necessary to control access on our computer systems and network security (NETSEC) is needed to control the security of our local area networks. Together, all of these concepts provide information security (INFOSEC).

What we do not have is any kind of certification process for computer systems that validates the security that is provided. Technology has simply progressed too fast for most of the proposed processes. The concept of a security Underwriters Laboratory has been proposed recently. The idea would be to have the lab certify the security of various

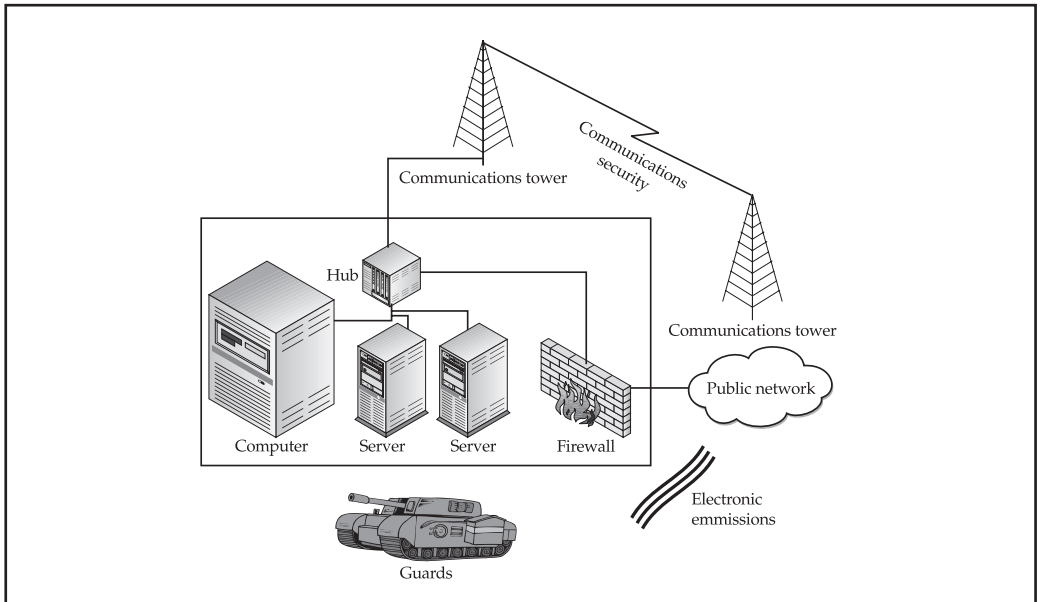

Figure 1-3. Information security includes many security concepts

products. If the product is not certified, users might be considered negligent if their site was successfully penetrated. Unfortunately, we have two problems with such a concept:

- The pace of technology continues so there is little reason to believe that a lab would have any better luck certifying products before they become obsolete than previous attempts.
- It is extremely difficult if not impossible to prove that something is secure. You are in effect asking the lab to prove a negative (that the system cannot be broken into). What if a new development tomorrow causes all previous certifications to become obsolete? Does every system now have to be recertified?

As the industry continues to search for the final answer, we are left to define security as best we can. We do this through good security practice and constant vigilance.

WHY SECURITY IS A PROCESS, NOT POINT PRODUCTS

Obviously, we cannot just rely on a single type of security to provide protection to an organization's information. Likewise, we cannot rely on a single product to provide all of the necessary security for our computer and network systems. Unfortunately, some vendors (in their zeal to sell their products) have implied that such was actually true. The reality of the situation is that no one product will provide total security for an organization. Many different products and types of products are necessary to fully protect an organization's information assets. In the next few paragraphs, we will see why some of the more prominent security product categories cannot be the all-encompassing solution.

Anti-Virus Software

Anti-virus software is a necessary part of a good security program. If properly implemented and configured, it can reduce an organization's exposure to malicious programs. However, anti-virus software only protects an organization from malicious programs (and not all of them—remember Melissa?). It will not protect an organization from an intruder who misuses a legitimate program to gain access to a system. Nor will anti-virus software protect an organization from a legitimate user who attempts to gain access to files that he should not have access to.

Access Controls

Each and every computer system within an organization should have the capability to restrict access to files based on the ID of the user attempting the access. If systems are properly configured and the file permissions set appropriately, file access controls can restrict legitimate users from accessing files they should not have access to. File access controls will not prevent someone from using a system vulnerability to gain access to the system

as an administrator and thus see files on the system. Even access control systems that allow the configuration of access controls on systems across the organization cannot do this. To the access control system, such an attack will look like a legitimate administrator attempting to access files to which the account is allowed access.

Firewalls

Firewalls are access control devices for the network and can assist in protecting an organization's internal network from external attacks. By their nature, firewalls are border security products, meaning that they exist on the border between the internal network and the external network. Properly configured, firewalls have become a necessary security device. However, a firewall will not prevent an attacker from using an allowed connection to attack a system. For example, if a Web server is allowed to be accessed from the outside and is vulnerable to an attack against the Web server software, a firewall will likely allow this attack since the Web server should receive Web connections. Firewalls will also not protect an organization from an internal user since that internal user is already on the internal network.

Smart Cards

Authenticating an individual can be accomplished by using any combination of something you know, something you have, or something you are. Historically, passwords (something you know) have been used to prove the identify of an individual to a computer system. Over time, we have found out that relying on something you know is not the best way to authenticate an individual. Passwords can be guessed or the person may write it down and the password becomes known to others. To alleviate this problem, security has moved to the other authentication methods—something you have or something you are.

Smart cards can be used for authentication (they are something you have) and thus can reduce the risk of someone guessing a password. However, if a smart card is stolen and if it is the sole form of authentication, the thief could masquerade as a legitimate user of the network or computer system. An attack against a vulnerable system will not be prevented with smart cards as a smart card system relies on the user actually using the correct entry path into the system.

Biometrics

Biometrics are yet another authentication mechanism (something you are) and thus they too can reduce the risk of someone guessing a password. As with other strong authentication methods, for biometrics to be effective, access to a system must be attempted through a correct entry path. If an attacker can find a way to circumvent the biometric system, there is no way for the biometric system to assist in the security of the system.

Intrusion Detection

Intrusion detection systems were once touted as the solution to the entire security problem. No longer would we need to protect our files and systems, we could just identify when someone was doing something wrong and stop them. In fact, some of the intrusion detection systems were marketed with the ability to stop attacks before they were successful. No intrusion detection system is foolproof and thus they cannot replace a good security program or good security practice. They will also not detect legitimate users who may have incorrect access to information.

Policy Management

Policies and procedures are important components of a good security program and the management of policies across computer systems is equally important. With a policy management system, an organization can be made aware of any system that does not conform to policy. However, policy management may not take into account vulnerabilities in systems or misconfigurations in application software. Either of these may lead to a successful penetration. Policy management on computer systems also does not guarantee that users will not write down their passwords or give their passwords to unauthorized individuals.

Vulnerability Scanning

Scanning computer systems for vulnerabilities is an important part of a good security program. Such scanning will help an organization to identify potential entry points for intruders. In and of itself, however, vulnerability scanning will not protect your computer systems. Each vulnerability must be fixed after it is identified. Vulnerability scanning will not detect legitimate users who may have inappropriate access nor will it detect an intruder who is already in your systems.

Encryption

Encryption is the primary mechanism for communications security. It will certainly protect information in transit. Encryption might even protect information that is in storage by encrypting files. However, legitimate users must have access to these files. The encryption system will not differentiate between legitimate and illegitimate users if both present the same keys to the encryption algorithm. Therefore, encryption by itself will not provide security. There must also be controls on the encryption keys and the system as a whole.

Physical Security Mechanisms

Physical security is the one product category that could provide complete protection to computer systems and information. It could actually be done relatively cheaply as well. Just dig a hole about 30 feet deep. Line the hole with concrete and place all-important systems and information in the hole. Then fill up the hole with concrete. Your systems and information will be secure. No one will be able to access them. Unfortunately, this is not a

reasonable solution to the security problem. Employees must have access to computers and information in order for the organization to function. Therefore, the physical security mechanisms that we put in place must allow some people to gain access and the computer systems will probably end up on a network. If this is the case, physical security will not protect the systems from attacks that use legitimate access or attacks that come across the network instead of through the front door.