CHAPTER I

INFORMATION SECURITY
VULNERABILITIES AND THREATS

A. Overview

As consumers in today’s market, we barely even think about the revolutionary developments that have occurred in recent years in electronic communications and commerce. It has become like driving a car or tying our shoes: simple and routine.

Click, and we’ve paid our mortgage for the month. Click, and we’ve submitted our taxes online. Click, and we’ve balanced our checking account. Click, and we’ve used a credit card to order pizza delivery.

We’ve gotten comfortable.

As legal professionals, however, information security concerns remain at the forefront of everyday business practice. Every week brings another headline decrying the latest large scale data compromise. Payment card accounts, Social Security numbers, and even medical records all are fundamental building blocks used by malicious hackers to facilitate identity and financial fraud. And every day, at every moment, from every corner of the planet, malicious and unauthorized intruders are attempting to breach systems to gather sensitive consumer data.

Data compromise alone does not represent the full scope of the threat. All too frequently, business organizations find themselves the victims of extortion, where hackers have gained full system level access to their networks and are threatening to shut down business operations unless and until the organization fulfills a ransom demand—holding a network hostage. In other scenarios, these malicious intruders gain access to one company’s network resources, only to launch attacks from those systems against other organizations. The methodologies, motivations, and vulnerabilities that drive computer-based crimes are so varied that obtaining a big picture understanding of the true nature and scope of the phenomena can be challenging.

A historical perspective on the nature of high tech crime also is paramount. While popular films from the early 1980s portrayed hackers as a disorganized group of bored suburban high school kids, the modern digital criminal is more daunting. Computer-based crime is highly focused, using specific vectors to attack specific targets to achieve specific goals. Within the last decade, high tech crime has become a highly organized and profitable affair—one that actively recruits fresh
talent to keep abreast of the latest security vulnerabilities and exploit
techniques.

As reflected by their actions and exploits, modern digital criminals
fully understand the fluid nature of information security and data
compromise. As information security techniques and methodologies
change over time, so do criminals’ methods of exploiting them.
Conversely, common practices within the information security industry
provide only static solutions that, more often than not, become irrelevant
within months, weeks, or even days. Even some solutions regarded as
industry best practices provide little more than emotional comfort for the
information security officers and systems administrators who implement
them.

Although the specific threats in the world of digital crime are always
changing, the fundamental elements of computer-based crime remain
constant: vulnerability, attack, exploit, and compromise of otherwise
restricted systems.

B. Technical Threats

The terms discussed in this section describe specific technical threats
to information security. Each of these threats functions by exploiting
known vulnerabilities within computer systems. Following each of the
terms presented are a description of the threat, the potential damage
posed by the threat, and the countermeasures that can help to protect an
organization from the threat. These solutions, however, are static in
nature and will remain relevant within only a limited timeframe as
technical threats continually evolve. Only by realigning the focus on
how businesses store sensitive data itself can government and industry
effectively remove the motivation that may be shared within the hacker
underground to breach systems.

1. Viruses

A virus is a computer program designed to attach itself to host files
and replicate repeatedly. Viruses attach to files so that they are activated
when the infected file executes (i.e., when the user opens the file).
Viruses are often configured to sit in a computer’s memory and infect
files as the computer opens, modifies, or creates new files. Similar to
human viruses, computer viruses usually display the following three
characteristics:
• **Self-Replication**: Computer viruses are designed to continually copy themselves onto multiple host programs or files, just like a human virus travels from one person to another.

• **Host Program or File**: Just like a human virus can survive only if it infects a living person, a computer virus must infect a host program or file.

• **User Activation**: A computer virus will not activate and replicate until a user executes it by clicking an e-mail attachment or visiting a malicious Web page.

a. **Potential Damage**

Viruses can harm computers by damaging programs, deleting files, or reformatting drive space. Some are not designed to do any damage at all, but simply replicate themselves and present text, video, or audio messages to the user. In addition, many viruses are poorly coded, leading to unintentional system crashes and data loss.

b. **Countermeasures**

One of the best ways to prevent a virus infection is to restrict the opening of e-mail attachments. E-mail attachments are the number one source for virus circulation. As many viruses usurp mailing lists from infected computers to redistribute themselves, even attachments from known or trusted sources can be dangerous. Another critical protective measure is to install and use antivirus software. All organizations should consider installing antivirus software as a matter of course and require by policy that such software run automatic updates and system scans on a routine basis.

2. **Worms**

A worm is a computer program that self-replicates and spreads like a virus without necessarily infecting a host file. Worms consist of independent codes that exploit known system vulnerabilities without the need for a user to activate them. They self-replicate and spread without any degree of user interaction. As a result, they often are able to spread faster than viruses. For example, the Structured Query Language (SQL)
Slammer worm, released on January 25, 2003, spread globally within minutes and resulted in costs of over $1 billion.

a. Potential Damage

A very common worm-based payload is the installation of a surreptitious “backdoor” in the infected computer, putting that computer under control of the worm author. “Sobig” and “Mydoom” are examples of such worms. Malicious criminals then use these “zombie computers” to threaten organizations with Denial of Service (DoS) attacks (i.e., attempts to make a computer resource unavailable to its intended users). In the case of the SQL Slammer, the worm was able to spread so prolifically that it caused major network outages all over the world.

b. Countermeasures

Like so many other threats, worms often can be effectively prevented through the use of antivirus software. Organizations should consider installing antivirus software as a matter of course and require by policy that such software run automatic updates and system scans on a routine basis.

3. Trojan Horses

The term Trojan horse is derived from Homer’s *Iliad*. Seeking to gain entrance to the fortified city of Troy, the Greeks built a large wooden horse near the beaches of Troy and then sailed away. After

2. Id.
3. The term “payload” refers to what a computer virus is programmed to do upon infection. Payloads can be programmed to unload the virus onto other computer systems, steal files or data, facilitate remote administrative access, or even destroy some or all of the data on the computer.
4. Refer to part B.9 of this chapter for a more in-depth discussion of “Denial of Service Attacks.”
5. See supra note 1.
Trojan soldiers brought the enormous horse into the city, Greek warriors emerged from the horse and overran Troy.

As it relates to computer security, the term describes a seemingly benign program or application that contains malicious code, unbeknownst to the victim. For example, a user might download and install what appears to be a harmless freeware game, but when the program is executed, it unleashes a payload that could erase data, install a keystroke logger capable of capturing everything a user types into the keyboard, or enable a remote hacker to access the victim computer.

a. Potential Damage

The potential harm from a Trojan horse is nearly limitless, constrained only by the imagination of the software’s authors. Once a system is infected with a Trojan horse, a malicious hacker often is able to obtain full “at the keys” access to the victim system. This ability facilitates keystroke logging, screen capturing, and any degree of data compromise resident on the victim system.

b. Countermeasures

Trojan horse programs cannot operate autonomously, as they depend on each new victim to activate them. Therefore, persons downloading or installing new software should exercise due diligence consistent with company policy, including thoroughly researching any product or application prior to installation. Because software and applications that install Trojan horses quickly earn a negative reputation on the Internet, a quick Internet search often can help to identify and discover these types of programs.

4. Botnets

A botnet refers to a collection of compromised or zombie computers running malicious programs under the control infrastructure of a remote commander. Commonly, the perpetrator of the botnet infrastructure has compromised a collection of remote systems using various malware and

6. “Remote commander” refers to the individual who controls the collected botnet computers remotely, usually for nefarious purposes.
7. “Malware” is slang for malicious software. Malware is software designed specifically to disrupt a computer system.