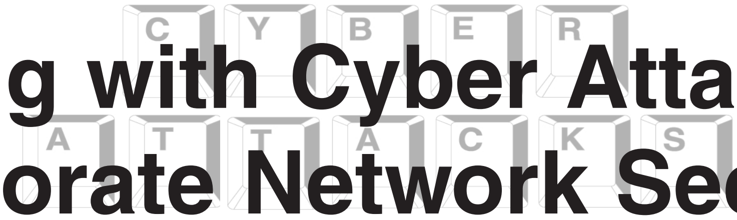

Dealing with Cyber Attacks on Corporate Network Security

Timothy A. Vogel

Is computer network security a job for lawyers? Yes! Network security involves fundamental issues of business risk and responsibility, on which attorneys advise clients every day.

COMPUTER SYSTEMS and networks are a mainstay of corporate America. Virtually every employee is provided with some type of computer access and an e-mail account, and companies deploy sophisticated computer networks in an effort to enhance worker productivity. Increasingly, these networks and systems are being connected to the networks and systems of other companies, and to the Internet. This activity raises a new set of threats and responsibilities for companies. As experts in risk assessment, loss prevention, and damage mitigation, attorneys are well positioned to help clients address and prepare for the risks inherent in doing business in cyberspace.

Timothy A. Vogel is a Director on the WorldCom Network & Facilities Legal Team. Before joining WorldCom he served as Deputy General Counsel of UUNET Technologies, Inc. The author wishes to acknowledge the groundbreaking work of Michael McGuire, Esq., Clint Smith, Esq., and the Netspionage working group of the American Bar Association in educating counsel on risks and issues associated with networked computer systems.

The purpose of this article is to raise awareness in the legal community of the nature and scope of the threat to networked computer systems, and to give attorneys the tools they need to get involved in crafting strategies for preventing and responding to these threats. Involvement of counsel in addressing network security issues is imperative because of the growing extent to which network security measures have implications for legal and business issues across the enterprise.

Attorneys have a personal and professional interest in this subject as well. For in-house counsel, there is an opportunity to add value and raise the profile of the legal department in the eyes of senior management. For outside counsel, there is an opportunity to raise these issues with clients, help them take steps to protect themselves, and counterbalance efforts by top accounting and consulting firms to claim this subject as their own.

THE NATURE OF THE THREAT • Threats to network security are real. Approximately 4,000 denial-of-service attacks happen weekly. *See*, ZD Net News, visited on July 2, 2001, 4:00 P.M. EDT, http://www.zdnet.com/zdnn/stories/news/0,4586,5092020,00.html.

High-profile attacks in the past year or so rendered targets as varied as Microsoft, the FBI, CNN, and Yahoo unreachable over the Internet for significant periods of time. *Id*. Press reports of cyber attacks are almost a weekly event. *See* System Administration, Networking, and Security Institute Newsbites Archive, visited on July 2, 2001, http://www.sans.org/newlook/digests/nbarchive.htm. In addition, the costs of preventing and responding to network security incidents are increasing.

In preparing for such attacks, there are two elements to consider; a perpetrator and a method of operation. On any given day, the perp in a cyber attack could be one of any number of folks.

Hackers and Crackers

"Hackers" is a term loosely used to describe folks that engage in cyber attacks for fun (or more precisely, some motive other than personal financial profit; "crackers" is the term generally used to describe folks who hack for profit). Hackers may be intrigued by the challenge. They may be genuinely interested in thwarting the latest in computer security technology, not to profit from it, but rather simply to know that they can best even the most sophisticated of security measures. Hackers also include teens and pre-teens that are just getting their first taste of hacking. Sometimes referred to as "script kiddies," these novices rely on drag-and-drop virus-creation software that permits them to easily assemble viruses at the click of the mouse.

Political Zealots

Political ideologues also pose a potential threat to networked computer systems. Your company's Web site is a bully pulpit for your enemies. For example, an upscale department store in the Washington D.C. area known for its selection of fine furs is surrounded by posters hung by anti-fur demonstrators. Those same folks would undoubtedly love to place those images on the company's Web site home page. The federal government understands this all too well. The list of government sites that have been altered or have been forced offline as a result of a hack includes the FBI, DOD, U.S. Senate, EPA, Energy Department, GSA, NASA, Fish and Wildlife, Interior Department and Park Service.

Foreign Governments, Competitors, and Investors

Foreign governments, competitors, and even investors are all interested in information possessed by American businesses. For example, the French have allegedly developed an espionage tool for intercepting communications, similar to the Echelon project largely believed to be undertaken by our own government. Wired, http://www.wired.com/news/politics/0,1283,44689,00.html; ZDNet, http://news.zdnet.co.uk/story/0,,s2079872,00.html. Whether any of the information gathered by the French government's efforts is shared with private industry is open to speculation.

Foreign governments or terrorist organizations could have more sinister aims as well. Hostile cyber attacks might target computer systems controlling power grids, municipal water supplies, air traffic control systems, or any other system the disruption of which would serve the perpetrator's aims. For example, in Australia, a man hacked into a computer-controlled waste management system and causing millions of gallons of raw sewage to spill out into local parks, rivers, and the grounds of a Hyatt Regency hotel. http://www.theregister.co.uk/content/4/22579.html. The *Washington Times* reports that in simulated "cyber war games," U.S. computer experts playing the part of foreign hackers managed to shut down all communications among the U.S. Pacific fleet, and could have shut down the entire western half of the U.S. power grid. *Washington Times*, June 22, 2001, http://www.washtimes.com/national/20010622-95748128.htm.

Finally, although competitors and investors are not likely to physically break into corporate offices, which of them would not be tempted to make a few login attempts at a corporate extranet site designed for use by that company's traveling sales personnel? An example of individuals going to great lengths for inside information can be found in the conduct of Charlie Sheen's character in the movie *Wall Street*, where Sheen moonlights with a cleaning company in order to obtain unfettered access to the files of corporate law firms in Manhattan.

Spammers

Spammers—individuals or companies engaged in the mass distribution of unsolicited e-mail—may view your client's systems as a handy source of additional computing power. Although the spammer is not primarily interested in harming your client or in damaging its systems, the act of sending a million e-mail messages through your client's mail server's open relay can bring legitimate corporate communications to a grinding halt as effectively as any denial of service or e-mail flooding attack. Similarly, use of an open relay can lend credibility to forged e-mail headers, thus tricking the recipient into thinking the e-mail came from someone it did not. An open relay on a mail server at the Federal Aviation Administration not only allowed spammers to send email through it but also allowed someone to send an e-mail with an faa.gov return address that looked like it originated on the FAA's system. The perpetrators could have sent forged emails from "faa.gov" and potentially disrupted airline traffic. http://www.newsbytes.com/news/01/172004.html.

Disgruntled Employees

Finally, lax security practices with respect to current and former employees can be a big source of risk. According to a Digital Research study, disgruntled employees and employee accounts that remain active after termination, present the biggest security threat to U.S. companies. More than half of respondents to an online poll indicated that their worst security breaches involved corporate users tapping into unauthorized information. The second biggest problem stemmed from user accounts that were left open after employees had left the company. *New York Times*, 20 June 2001, http://www.nytimes.com/reuters/technology/tech-tech-security-su.html.

HOW THEY DO IT • Knowing who might be out to get your client is only the lesser half of the battle. The more important questions are how are they doing it and what can be done to stop them. Loosely speaking, cyber attackers usually seek to access corporate systems, access corporate data, or disrupt the victim's ability to do business. Often the goal is a combination of these.

Access to Systems

Access to corporate systems permits an attacker to use those systems for his (or her) own ends. For example, a compromised computer server could be used as a launch platform for a subsequent attack on a different system. Not only would this permit the attacker to benefit from the computing power of multiple third-party systems, it would make tracing the attack more difficult, as all cyber roads would lead to Rome, or some other spurious destination of the attacker's choosing. To identify a third-party server that might be vulnerable to an attack, one could use a variety of tools such as war dialers and port scanners. These devices could quickly contact multiple computer systems and identify computers connected to the network that are vulnerable to an attack. War dialers would do this by dialing numbers that lead to computer modems. Once a computer answers, it usually offers a login prompt, and thereby gives the attacker an opportunity to attempt to gain access. Port scanners generally use standard network tools—the same tools used by legitimate network administrators—to identify which services (FTP, web servers, etc.) are running on a server simply through review of information provided automatically by the scanned server in response to the attacker's automated request. Once an attacker identifies a server or set of servers that "have their ears on," she can frequently ascertain the operating system or web server software in use, and then proceed to try to exploit any one of a number of known vulnerabilities with respect to that system or software.

Physical Access

Similarly, access to company networks can be gained through physical access to machines connected to those networks. In most cases, a company's computers are physically located in secure, non-public areas of the company's premises. However, laptop computers are frequently stolen. These computers are often configured to automate the login process to a great extent. In most cases, the only piece of information an employee needs to provide to log in is a password (and that piece of information is not infrequently found affixed to the computer itself, or only slightly less accessible, on a piece of paper in the case in which the stolen computer was stored).

Social Engineering

Finally, access to company systems is frequently gained through social engineering. At its simplest level, this could involve an attacker obtaining an employee's username and password through a phone call on which the attacker pretends to be someone in the company's computer department who needs to know that information for some routine system maintenance. At a more sophisticated level, social engineering takes place in the form of e-mail attachments. The Melissa and Love-Bug trojans were examples of attackers convincing employees to take actions that proved harmful to the employee's and company's best interests. More sophisticated e-mail attachments could install keyboard sniffers or backdoors on employee computers. Ultimately, social engineering may prove to be the most difficult "system" vulnerability to fix. The strongest security system cannot prevent an attack perpetrated through persons who are explicitly, by system design, granted access to it.

Access to Information

Once an attacker has access to company systems, she may desire to exploit, destroy, or prof-