

The COMPUTER & INTERNET *Lawyer*

Arnold & Porter, Editor-in-Chief

Cyber-Security Liability: Is It Time to Get Off the Soapbox?

By **Beryl A. Howell**

The federal approach to cyber-security has been called the “soapbox strategy”: issue warnings on the urgency of the problem, urge hardware and software manufacturers to make more secure products, and cajole owners and operators of critical business networks and utilities to devote more attention and resources to their own cyber-security.¹ Rather than impose affirmative obligations on manufacturers, owners, or operators of computer systems and software to take responsibility for cyber-security, these parties have been shielded from liability that might serve as an incentive to take action.

Lacking any sticks to force protective action, the Department of Homeland Security is left with outreach props, like declaring October 2004 “National Cyber Security Awareness Month” to stress the importance of cyber-security. At the same time, Internet-related computer security incidents have become so commonplace and have reached such a large scale that CERT/CC² is no longer publishing the number of such incidents but instead is using alternative metrics.

Policy makers and legislators are regularly bombarded with statistics on the scope of the cyber-security problem. The Financial Services Roundtable told Congress that software vulnerabilities approach a cost of

\$1 billion annually to the financial services industry.³ Even when system software and hardware work as intended, sloppy design and lax system administration create vulnerabilities that are easily exploitable by malicious code, denial of service attacks, and other forms of electronic crime. One recent survey reported that electronic crime cost organizations about \$666 million in 2003 alone.⁴

In short, the dual-pronged approach of liability protection and exhortation to improve the security of private sector computing environments is failing, making it more likely that policy makers’ attention may shift to passing meaningful legislation that gets the job done. Recent security breaches resulting in the unauthorized disclosure of personal information held by Choicepoint and the loss of personal information by Bank of America, including information for members and staff of the US Senate, have made this issue more pressing inside the halls of Congress.⁵

From the vantage point of investigating cyber-security incidents, technical service firms regularly see the economic harm to businesses caused by cyber-security breaches, as well as how frustrating and distracting such incidents can be for the senior management at Fortune 500 companies. In one recent case solved by the firm of this author, a company was the victim of a two-year email harassment campaign in which its clients were sent emails with obscene attachments and derogatory information about the company. As those clients started taking their business elsewhere, the company involved the FBI but was unable initially to identify who was sending the emails or even whether the emails were being sent by a person acting alone or a group of people.

Beryl A. Howell is the Managing Director and General Counsel of the Washington, DC, office of Stroz Friedberg, LLC, a technical services and professional consulting firm specializing in digital forensics and cyber-security investigations. This article is adapted from the author’s presentation at the ABA Annual Meeting in August 2004.

Security

Tracking the perpetrator was no easy matter since he had used several methods simultaneously to hide his identity. He had spoofed the email address to make the emails appear to come from senior executives within the company; he had hijacked AOL and Yahoo! email accounts with stolen passwords from authorized users to send the spoofed emails; and he had used open computer labs at universities and unprotected wireless access points to access the Internet to transmit the emails. The email harassment escalated to a multimillion dollar extortion demand on the Chief Executive Officer of the company, or else the perpetrator threatened to unleash a denial of service attack on the firm's clients to make it appear to come from the company.

A variety of technical and investigative techniques employed by the author's firm aided in tracking down the culprit in three months. He pleaded guilty and was sentenced in federal court for violations of the Computer Fraud and Abuse Act (CFAA).

This investigation revealed multiple forms of physical and cyber-security vulnerabilities that allowed this criminal to steal confidential data, not just from hacking into the company's computer network by using obsolete but still viable authentication passwords and tunneling into the corporate network due to configuration flaws but also by "dumpster diving" or physically going through the company's unsecured trash bins. He used multiple wireless routers that consumers are setting up in their homes without changing the default settings to secure access and log users and insecure computer labs at local universities. The defendant was deftly able to exploit multiple vulnerabilities for criminal purposes and cause real economic harm to a company.

While the victim company did not seek redress from the universities or the homeowners with open wireless access points through which the perpetrator launched his attacks, it seems only a matter of time before such a suit is brought on the theory that lax security, that is, negligence, by the innocent entity in the middle made the attack possible. Allocating who will bear the cost of cyber-security losses and when the cost burden should be shifted from the victim to others is a time-honored way in our legal system to force change and focus attention and resources on fixing problems. Yet, this allocation has been directed away from computer software and hardware manufacturers, due to a federal trend of providing liability immunity, as demonstrated by three fairly recent examples of federal legislation.

Y2K Act

Five years ago, when Americans were worried about Y2K computer failures, Congress passed a liability-limiting law that created special procedural hurdles for

plaintiffs who claimed either actual or potential computer failures that caused harm before January 1, 2003. This law preempted state consumer protection laws, capped punitive damages, and limited liability for any potential Y2K failures regardless of how much harm or injury was foreseeable or caused.⁶ Opponents, who were concerned that this law promoted a "don't worry, be happy" mentality instead of providing incentives for software manufacturers to take remedial action and fix the problems, lost this debate in the Congress.

In fact, the new law had the effect of allowing a software manufacturer to avoid certification of a plaintiff class of software consumers, after the manufacturer cancelled technical support for a software product with a known Y2K defect, rather than repair it.⁷ Other plaintiffs who claimed harm from software with Y2K defects also had their suits dismissed for failure to satisfy the new pleading requirements under the Y2K Act or stayed with mandatory referral to alternative dispute proceeding.⁸

CFAA

Y2K may have been a one-off event, but subsequent laws similarly redirect liability for cyber-security failure away from manufacturers. The CFAA is the primary federal criminal statute prohibiting multiple forms of computer crime, including computer fraud, viruses, worms, theft of computer data, and hacking. This statute has ridden the wave of concern about cyber-security over the past 20 years, with periodic amendments, which have dramatically expanded its reach. Tracking these changes, and in particular, the scope of the civil liability provided in this law, illustrates the trends generally at the federal level.

When enacted, the CFAA focused on outside hackers or malicious insiders who obtained unauthorized access to classified information or other information on government computers. The only private data and computers deemed sufficiently important to protect were financial records or credit histories held by financial institutions. There was no civil liability, no specific federal prohibition on damaging computers or stealing data from computers, or any general federal protection for private sector computers. Since then, Congress has regularly amended the CFAA to expand its scope to virtually every computer connected to the Internet, to provide civil causes of action for violations, and to create new offenses for online extortions, damage, or alteration of data by unauthorized users, the theft of data, and the transmittal of damaging worms, viruses, or other programs.

One byproduct of the new offenses, in combination with authorizing civil liability, was the use by software consumers of this statute to sue software and hardware manufacturers for defective or negligently designed prod-

ucts. As one court explained, in allowing a civil suit under the CFAA to proceed against the manufacturer of faulty computer parts, “Congress, grappling with technology that literally changes every day, drafted a statute capable of encompassing a wide range of computer activity designed to damage computer systems—from computer hacking to time bombs to defective microcode.”⁹

Following the 9-11 terrorist attacks, Congress amended the CFAA to increase penalties for abuse of and to provide additional protections for government computers. At the same time, a little-noticed but significant provision of the USA PATRIOT Act limited the scope of civil liability for software or hardware glitches so that no civil action may be brought under the CFAA for the “negligent design or manufacture of computer hardware, computer software, or firmware.” This provision limits the ability of consumers, including businesses, to sue for alleged security vulnerabilities in software or hardware that may have resulted in loss.

One commentator acknowledged that, “[a]dmittedly, Congress seems to have intended the CFAA to curb computer fraud and abuse resulting from unauthorized computer use. Removing manufacturer liability is faithful to the original purpose.” Nevertheless, “the unfortunate result was to foreclose an opportunity for software manufacturers to be held liable for defective programming.”¹⁰

Critical Infrastructure Information Act

Other recently enacted federal laws continue this incentive and liability limiting approach. For example, the Critical Infrastructure Information Act, passed as part of the Homeland Security Act in 2002, granted special protections to information voluntarily submitted by businesses to any federal government agency when that information is marked as “critical infrastructure information” (CII). This law was intended to make moot the excuses that businesses used to explain their reluctance to share with the government information about cyber-security vulnerabilities and security risks to systems supporting energy, banking, telecommunications, transportation, and other vital services, most of which are owned and controlled by the private sector.

The CII Act provides private sector CII-marked information with more protection than classified national security information. CII-marked information is exempt from Freedom of Information Act disclosure, exempt from rules barring submission of *ex parte* materials to regulators, exempt from federal Advisory Committee Act rules, and exempt from disclosure to Congress. Criminal penalties apply to any government worker who discloses CII-marked information. Moreover, CII-marked information may not be used

directly in any civil action, even against persons other than the submitter, without the submitter’s consent.

The number of CII-marked submissions has been “underwhelming,” with only a handful of submissions made between January and May 2004.¹¹ Clearly, the carrot that the government is offering to industry is insufficient inducement for voluntary disclosure. The next resort may be mandatory disclosure, which is the direction taken by at least one state and in pending federal legislation.

Trends

The current liability limitations at the federal level reflect only a Pyrrhic victory for software and hardware manufacturers. Consumer pressure for improved privacy protection is forcing a new trend. States are responding by enacting a patchwork of regulations and new laws.

California has taken the lead to shift the burden of security risks to those owning and operating computer systems and networks. The recent California mandatory disclosure law (SB 1386) requires companies holding computerized personal information of California residents to take steps either to encrypt this personal information or adopt, as part of an information security policy, notice and disclosure procedures for any computer security breaches, whether or not the breach occurs in California. Noncompliant companies are subject to civil suits, including class actions, for damages and injunctive remedies in California courts. One commentator observed that, “in forcing companies to come clean, the California law takes the opposite approach of the Bush Administration’s emerging cyber-security policies, which encourage secret disclosure to government officials, rather than public warnings.”¹²

Similarly, state attorneys general and the Federal Trade Commission are using unfair practices laws in enforcement actions against companies for data leakages on Web sites and misleading consumers about the security and privacy afforded their data.

A federal version of the California mandatory disclosure law is pending to require federal agencies and companies possessing electronic data with personal information to disclose any unauthorized acquisition of such unencrypted information by notifying the persons whose personal information was affected. Other pending bills targeted at spyware would require disclosure to computer users of certain computer software features that may pose a threat to user privacy.

Against the backdrop of cyber-terrorism fears, escalating cyber-security losses, and privacy concerns, the soapbox strategy may not provide sufficient assurance that cyber-security vulnerabilities are being addressed effectively and expeditiously. The National Academy of Sciences has noted:

Security

Policy makers should consider legislative responses to the failure of existing incentives to cause the market to respond adequately to the security challenge. Possible options include steps that would increase the exposure of software and system vendors and system operators to liability for system breaches and mandated reporting of security breaches that could threaten critical societal functions.¹³

Alternative approaches being suggested include:

- Providing tax incentives to increase network security expenditures or to obtain cyber-security insurance, using the marketplace to encourage implementation of best cyber-security practices for lower premiums;
- Requiring distribution of computer software and hardware with the most secure default settings activated;
- Enhancing the investigative and technical tools and procedures available to identify and track malicious online activity and actors;
- Imposing liability on manufacturers or network operators for negligent actions or omissions that enable widespread harm to others; and
- Requiring disclosures by public companies of potential cyber-risks or actual security breaches in their annual Form 10-K disclosure.¹⁴

It is only a matter of time before federal policy makers get off the soapbox and start legislating more aggressive measures.

Notes

1. Michael A. Vatis, Testimony before the US House of Representatives Committee on Government Reform, Subcomm. on Technology, Information Policy, Intergovernmental Relations and the Census, at hearing on "Cybersecurity: The Challenges Facing our Nation in Critical Infrastructure Protection," Apr. 8, 2003, at p. 5-6.
2. CERT/CC is the Computer Emergency Response Team Coordination Center at Carnegie Mellon University that monitors computer security problems and solutions and states on its Web site, "Given the widespread use of automated attack tools, attacks against Internet-connected systems have become so commonplace that counts of the number of incidents reported provide little information with regard to assessing the scope and impact of attacks. Therefore, as of 2004, we will no longer publish the number of incidents reported." See <http://www.cert.org/stats/>.
3. Louis F. Rosenthal, Testimony before the US House of Representatives Committee on Government Reform, Subcomm. on Technology, Information Policy, Intergovernmental Relations and the Census, at "Oversight Hearing," June 2, 2004 (written statement, p.3).
4. 2004 E-Crime Watch Survey, CERT Coordination Center, CSO Magazine and US Secret Service, p.6.
5. Jon Swartz and Sandra Block, "Underground Market for Stolen IDs Thrives," *USA Today*, Mar. 3, 2005; Jim Snyder, "Congress looking into ways to shore up privacy of data," *The Hill*, Mar. 2, 2005.
6. Y2K Act, P.L. 106-37 (July 20, 1999), codified at 15 U.S.C. § 6601, *et seq.*
7. Mineral Area Osteopathic Hospital, Inc. v. Keane, Inc., 192 F.R.D. 589 (N.D. Iowa 2000).
8. Lewis Tree Service, Inc. v. Lucent Technologies, Inc., 2000 U.S. Dist. LEXIS 12922 (S.D.N.Y.); Preferred MSO of America-Austin v. Quadramed Corporation, 85 F. Supp. 2d 974 (C.D. CA 1999).
9. Shaw v. Toshiba America Information Systems, Inc., 91 F. Supp. 2d 926, 937 (E.D. Tx 1999); North Texas Preventive Imaging, L.L.C. v. Eisenberg, 1996 U.S. Dist. LEXIS 19990 (C.D. Cal. Aug. 19, 1996) (finding that plaintiff had stated claim under § 1030(a)(5)(A) when disk manufacturer had provided plaintiff with defective disks that were programmed to render software inoperable on a specific date); In re AOL Version 5.0 Software Litigation, 168 F. Supp. 2d 1359 (S.D. Fl. 2001) (plaintiff's consumers stated claim under CFAA for injury from defendant's defectively designed and/or unreasonably dangerous software installation process).
10. Kevin R. Pinkney, "Putting Blame Where Blame is Due: Software Manufacturer and Customer Liability for Security-Related Software Failure," 13 *Albany Law Journal of Science & Technology* 43, 65 (2002).
11. William Jackson, "Response Slow to DHS Protected Info Sharing," May 24, 2004, GCN Staff, available at http://www.gcn.com/vol1_no1/security-policy/26030-1.html.
12. Kevin Poulsen, *Security Focus*, Jan. 6, 2003.
13. National Academy of Sciences, National Research Council, Computer Science and Telecommunications Board, "Cyber-security Today and Tomorrow: Pay Now or Pay Later," (2002).
14. M. A. Vatis, *supra* n.1.

Reprinted from *The Computer and Internet Lawyer*, Volume 22, Number 5, May 2005, pages 1-4, with permission from Aspen Publishers Inc., A WoltersKluwer Company, New York, NY 1-800-638-8437, www.aspenpublishers.com