

Cyber Tech Litigation Report

Box 62090 • King of Prussia, PA 19406-0230 • (610) 768-7800 • fax (610) 962-4991

Viruses, Hackers And Outages:

Who Pays?

Federal Court Rules That Business Interruption Insurance Covers Loss Of Computer Functionality

by
Mark Slater, Esq.,
John Pernick, Esq.,
Jonathan Hersey, Esq.

Sonnenschein Nath & Rosenthal
San Francisco, California

**A commentary article
reprinted from the
June 2000 issue of:
Mealey's
Cyber Tech Litigation Report.**

Commentary***Viruses, Hackers And Outages: Who Pays?******Federal Court Rules That Business Interruption Insurance Covers Loss Of Computer Functionality***

By

Mark K. Slater

John D. Pernick

Jonathan P. Hersey

[Editor's Note: Mark Slater is a partner in the Intellectual Property and Technology Department in the San Francisco office of Sonnenschein Nath & Rosenthal. John Pernick and Jonathan Hersey are associates in the firm's San Francisco office and are members of the firm's Intellectual Property and Technology Department. Copyright 2000 by the authors. Responses to this article are welcome.]

There are three kinds of death in this world. There's heart death, there's brain death, and there's being off the network.

— Guy Almes

A company's most valuable assets — information and access to information — reside on its computers. For web businesses, computers are the very life's-blood of their existence. But these systems are vulnerable: Today's saboteurs have traded their wooden shoes for keyboards.¹ And the internal damage to computers caused by viruses and hackers is devastating. Fortunately, a recent federal court confirms that relief for the loss of computer access and functionality caused by computer viruses, hacker attacks and power outages may be found in business interruption insurance policies.

Like any valuable property, computer networks can be damaged. Consider:

- The recent "I Love You" computer virus, which searches its host computer and overwrites most graphic and music files. The virus replicates itself by sending an e-mail with an infected file to all persons listed in the user's address books, and by sending an HTML version of the virus to anyone who connects to the user's IRC chat server.² Computer economics experts estimate the "I Love You" virus may have caused between \$5 and \$10 billion of damage.³
- In February 2000, several major Internet companies, including Yahoo!, eBay, E*Trade, and Amazon were crippled by hacker(s) unknown who flooded these web sites with false requests for information.⁴ These "denial of service" attacks overwhelmed the websites' servers and blocked most legitimate business to the web sites.

- In March 1999, the "Melissa" virus appeared as an e-mail attachment innocently labeled "list.doc." The virus propagated itself by sending an infected e-mail to the first 50 addresses in the user's address book. The immense proliferation of e-mails and fear of spreading the virus to customers caused many corporations, like Intel, to shut down their mail systems altogether.⁵
- Less sinister but equally troubling was a December 1998 power outage in San Francisco that crashed the computers at the Pacific Stock Exchange, halting stock and options trading in the 800 stocks handled solely by the San Francisco branch of the exchange.⁶

Law enforcement agencies work to apprehend computer criminals. Programmers design and upgrade software to protect and preserve computer functionality. But from a company's perspective, the loss of computer access — whether from a virus, hacker, power outage or other source — still amounts to a costly interruption of business. The question then is how companies can recover losses caused by these and future interruptions.

One potential avenue for recovery is business interruption, or BI, insurance. Generally, BI insurance is designed to reimburse for the actual loss of profits a company sustains as a result of unforeseen suspension of its operations. While each BI policy's coverage, deductibles and exclusions are different, most BI policies require that business be interrupted due to direct physical loss of or damage to property. A business interruption caused by fire would be covered, while lost profits due to a poor market would not. If the fire destroyed the business' computers, the interruption caused by that loss would also be covered. However, when a company cannot do business because its computer network has been rendered inoperable as a result of lost or corrupted programming, the damage is as real as any caused by fire.

One federal court recently determined that the loss of use, access to and functionality of a company's computers constitutes physical loss or damage covered by its BI insurance. In *American Guarantee & Liability Insurance Company v. Ingram Micro Inc.*, a power loss occurred at an Ingram Micro computer facility in Arizona responsible for data processing and data base maintenance operations.⁷ The power outage in Arizona lasted only a few minutes, but the loss of programming information caused by the outage resulted in substantial lost business. Ingram Micro made a claim under its BI insurance policy. The insurer denied the claim and filed suit against Ingram Micro, alleging that the computers were not "physically" damaged by the power outage.

Ingram explained in its court papers that computers, and their programming information are physical. The programming instructions that direct the computer are stored in the computer's Random Access Memory, or RAM. The instructions are written in an alphabet of 1's and 0's, which correspond to differences in voltage resident in the electronic switches that make up the RAM. When power is cut off to the computer, the differences in voltage and the specially programmed 1's and 0's disappear. When power is restored, the switches are all reset to 0. The programming information that had been physically stored in the computer's RAM is lost. Until this programming is restored, the computer cannot function properly. Thus, the loss of power causes a physical change to the computer that can render it inoperable. "Computerspeak," responded the insurer in its court papers.

The court found: "[a]t a time when computer technology dominates our professional as well as our personal lives . . . 'physical damage' is not restricted to the physical destruction or harm of computer circuitry but includes loss of access, loss of use, and loss of functionality." The court found support for its conclusion in several federal and state statutes. The federal computer fraud statute defines "damage" as including "any impairment to the integrity or availability of data, a program, a system, or information."⁸ In Connecticut, a person is guilty of a computer crime when he "disrupts or degrades or causes the disruption or degradation of computer services."⁹ Similarly, under New York law, a person is guilty of computer tampering when he "intentionally alters in any manner or destroys computer data or a computer program of another person."¹⁰ The court concluded: "Lawmakers around the country have determined that when a computer's data is unavailable, there is damage; when a computer's services are interrupted, there is damage; and when a computer's software or network is altered, there is damage. Restricting the [BI insurance policy's] language to that proposed by [the insurance company] would be archaic."

Companies today depend on and are defined by their computers and electronic networks. Damage to their programming can cost a business more than a fire or flood. Fortunately, BI insurance may provide the means to recover lost profits from the damage that impairs the intended use and functionality of a company's computer systems.

ENDNOTES

1. In 1897, disgruntled French workers tossed their wooden shoes (sabots) into factory machines to interrupt production. Hence, "sabotage."
2. Information Bulletin, K-039: *VBS.Loveletter.A Worm*, Computer Incident Advisory Capability, May 5, 2000; <<<http://ciac.org/ciac/bulletins/k-039.shtml>>>.
3. IJ News Service, "Love" Virus Cost Put at \$10 Billion, Marin Independent Journal, May 7, 2000; <<<http://www.marinij.com/news/archive/Saturday/stories/news3000370.shtml>>>. Computer Economics of Carlsbad, California, has determined that of the estimated 45 million people who received the "I Love You" bug, half lost access to e-mail and potential business because their e-mail systems needed to be taken off-line. *Ibid.*
4. Michael Brick, *National Discount Brokerage Faces Hacker Attack*, NYTimes.com, Feb. 24, 2000; <<<http://www.nytimes.com/library/tech/00/02/biztech/articles/>>>.
5. Kathleen Ohlson & Ann Harrison, "Melissa" Mutates, Computerworld Online News, Mar. 29, 1999; <<<http://www.computerworl.com/home/news.nsf/all/9903291melissa2>>>.

6. Sam Zuckerman, *Pacific Exchange Power Crash; Most Other Financial Institutions Stay Open*, San Francisco Chronicle, Dec. 9, 1998; <<<http://www.sfgate.com/cgi-bin/article.cgi?file=/chronicle/archive/1998/12/09/BU75828.DTL>>>.
7. United States District Court for the District of Arizona [Tucson Division], Civil Case No. 99-185 TUC ACM, filed April 15, 1999. The authors represent Ingram Micro Inc. in this action.
8. 8 U.S.C. § 1030 (West 1999).
9. Conn. Gen. Stat. Ann. § 53a-251 (2000).
10. N.Y. Penal Code § 156.20 (McKinney 1999). ■



4

5



6

7

