

By Robert Steinberg

Advising Clients about Hacker Insurance

Breaches of computer network security can lead to significant liabilities for companies

The financial losses facing corporate America as a result of network security breaches are staggering—hundreds of millions, if not billions, of dollars each year.¹ A 2002 joint survey by the FBI and the Computer Security Institute estimates that losses for just 44 percent of the 503 survey participants—primarily, large U.S. corporations—already exceeded \$455 million, with the theft of proprietary information and financial fraud representing the two most serious categories of losses (\$170 million and \$115 million, respectively).²

The reality is that these estimates, however considerable, likely represent only the tip of the iceberg, given that companies continue to notoriously underreport network attacks while apparently paying millions in hush-hush out-of-court settlements. Indeed, the financial toll from network breaches mounts each year as a result of threats originating within and outside the firewall, including: 1) viruses, worms, and Trojan horses, 2) system penetration or unauthorized access, 3) denial-of-service attacks, 4) theft of computer transaction information, including confidential customer data, 5) cyber-extortion, and 6) vandalism.

These losses should ensure that attorneys do a better job of educating their clients about the true magnitude of the risk confronting them as well as the key role that new insurance products—known as network-risk, hacker, or cyber policies—can play in protecting company interests. In fact, informed legal guidance is certain to become indispensable for many clients in the 2003 insurance renewal cycle, when many general policies—such as CGL, D&O, E&O, and property—will expressly disclaim losses resulting from network breaches, including those from viruses and e-vandalism. This will leave many clients dangerously exposed and forced to scramble to choose among the available coverage options and vehicles.

By all indications, corporate America continues to misunderstand the dynamics of the network security problem. For example, executives appear to believe that so long as their core business is not dependent on pure e-commerce, their companies remain insulated from significant losses from network security breaches. The reality is that most companies are reliant on some form of in-house technology for transacting important company business. Company computers might be shielding key assets or trade secrets, maintaining or retrieving customer data, providing customer service, or coordinating widespread business operations. Another common misconception is that existing technology alone—such as firewalls, virus software, intrusion detection devices, and encryption systems—can provide sufficient protection. While this technology can help defend against network breaches, it cannot eliminate the risk.

The dangers facing uninformed corporate clients are not simply the result of direct first-party losses from lost income. Companies also face the risk of third-party claims arising from the companies' failure

to maintain proper network security. The scenarios leading to third-party damages abound. For example, hackers launching malicious code into company networks can expose confidential customer information to the public—including credit card numbers—which can lead to claims against a company by its own customers. In a denial-of-service attack, hackers hijack one company's computer system to launch an attack against a second company, redirecting the first company's traffic to the second's site and overwhelming the second company's servers. This increasingly familiar scenario can lead to a claim by the second company against the first company for inadequately securing the technology that led to the second company's loss.

Stand-alone network-risk, hacker, or cyber insurance is now being offered by numerous big-name insurers. Depending on the selected coverage, these policies offer protection against intangible data loss from viruses, denial-of-service attacks, and theft of consumer information—and the protection can extend to third-party liabilities. Insurance premiums remain considerable, and prequalifying security assessments can be demanding; moreover, legal advice is often a prerequisite for navigating the various gaps and exclusions written into such policies.

Clearly attorneys cannot afford to leave network security to a client's IT department. Practitioners cannot simply become involved only after a loss when the client needs to either defend against or settle a hefty claim. Clients must be advised to be proactive on security.

Moreover, hacker insurance may be a nearly indispensable business tool. For corporations with well-known brand names, in high visibility industries, with significant Web presences, or sensitive information, a single breach, with the potential for third-party claims, can be financially devastating. For companies less likely to be targets, especially those that cannot easily afford the cost of hacker insurance, practitioners can advise a strategy of self-insurance via technology and procedural upgrades. Either way, the bottom line is that companies need legal guidance. ■



Robert Steinberg, a partner in the Los Angeles office of Latham & Watkins, focuses his practice on transactions and litigation involving technology and media.

¹ The author wishes to thank Latham & Watkins associate Ilana Makovoz for her assistance with this article.

² COMPUTER SECURITY INSTITUTE/FBI, 2002 COMPUTER CRIME AND SECURITY SURVEY, available at www.gocsi.com.