Is Your Company Protected? Developing a Comprehensive Cyber-Security Plan to Mitigate Legal Exposure From Cyber-Crime

by D. Jean Veta, Paul W. Schmidt & Rochelle E. Rubin *

Introduction

As use of the Internet has spread, businesses must now consider whether their online services are protected against cyber attacks and the resulting legal exposure that can result from such attacks. Smart businesses address these concerns by regularly revising and updating a comprehensive cyber-security plan. The reason is simple.

Computer crime, also known as cyber-crime, is a growing and increasingly costly phenomenon.[1] The first half of 2002 saw a 28% increase in internet attacks, with more than 180,000 of them successful.[2] In a recent study, the Federal Bureau of Investigation and the Computer Security Institute[3] reported that 90% of corporate and other respondents detected some type of computer breach in the prior year.[4] Although only 44% of these respondents specified a loss amount, the quantified losses from computer security breaches exceeded $455 million.[5]

Computer crime, also known as cyber-crime, is a growing and increasingly costly phenomenon.

With the creation of about fifty new computer viruses weekly and the increasing sophistication of hackers,[6] the FBI estimates that actual losses by businesses across the United States reach well beyond the $7 billion mark.[7] Recent concerns over terrorists targeting key industries—whether utilities, emergency services, or even, more broadly, financial services—add a frightening new dimension to the liability picture.[8]

As a result of these high costs, losses from acts such as online theft of confidential data, denial of service attacks, and computer viruses are frequently discussed, as are the technical measures to guard against such losses. However, little, if any, attention is devoted to what is becoming an equally serious problem: a company's legal exposure resulting from a cyber attack. This article describes this potential legal exposure and offers suggestions on designing an effective cyber-security plan to mitigate such exposure.

Understanding Legal Exposure from Cyber-Crime

Cyber-crime is a far-reaching problem, often harming parties other than the company targeted by the attack. Employees, customers, business partners, investors, and others may find themselves indirectly victimized by the same singular act of cyber-crime. For a targeted company, the costs of cyber-crime include not only the loss of business arising from, for example, the debilitation of its network systems, but also the expense of defending against lawsuits brought by indirect victims seeking to recover their own cyber-crime-related losses. Targeted companies in certain industries may also confront additional costs from cyber-crime including risk of exposure to regulatory actions brought by various government agencies for, among other things, failure to take adequate security precautions to prevent the harm from spreading to others.

[L]ittle, if any, attention is devoted to what is becoming an equally serious problem: a company's legal exposure resulting from a cyber attack.

Although few lawsuits in this context have emerged to date,[9] the incentives for bringing such claims are clear: targeted companies are more easily identified than cyber-criminals, they are much less likely to be judgment-proof, and the party seeking to recover can almost always argue that the company could have taken some additional security measure that would have prevented the loss. Given existing causes of action under which such claims could arguably be brought and the potential recovery available, these claims

* *D. Jean Veta is a partner in the law firm of Covington & Burling whose practice focuses on cyber-security issues, internal investigations, and other civil and criminal enforcement matters. Paul W. Schmidt is an associate at Covington & Burling and Rochelle E. Rubin is a former associate who is now an Assistant United States Attorney at the U.S. Attorney's Office for the District of Columbia.*

©2002 GLASSER LEGALWORKS

appear imminent, creating significant legal exposure for companies that have failed to develop and implement comprehensive cyber-security plans.

Liability to Customers for Loss of Confidential Data

In today's litigious society, businesses can be assured that at some point some customer, whether an online or in-store patron, will bring suit for perceived wrongs. And in this new age of increased interconnectedness, one type of wrong is particularly likely to give rise to lawsuits—a company's failure to protect confidential customer information from theft by cybercriminals (*e.g.*, hackers stealing credit card numbers).[10] Companies can anticipate such suits becoming increasingly common as consumers become ever more aware of the potential risk and real-world losses[11] associated with cybertheft. A company's exposure is further increased by the availability of class action lawsuits and their prospect for significant damages, litigation costs, and adverse publicity.

Customers bringing suit for theft of their confidential data, such as credit card information or customer profiles,[12] may claim that the company breached express or implied contractual obligations by not safeguarding the data properly. Absent a preexisting contractual relationship, customers alternatively may seek to recover compensatory and punitive damages based on a tort theory of negligence. To make out a claim of negligence, customers would argue that the defendant-company owed them a duty of care, that the company breached this duty by not safeguarding the customer data stored on its network, and that the breach proximately caused the theft and accompanying loss.[13] Although the thief's intervening act presents a problem in proving that the business's protection systems caused the customers' harm, plaintiff-customers might attempt to overcome this difficulty by arguing that computer hacking is foreseeable in light of high cyber-crime rates and widespread awareness of these rates.[14]

Companies also may face legal liability in instances where the customer information is not stolen directly from their network. For example, liability may arise if a company shares customer data with a non-secure source from which the data is then stolen.[15] Similarly, a company's failure to take steps to prevent wrongdoers from setting up web sites that are misleadingly similar to that company's site may give rise to liability if customers then erroneously transmit confidential data to the masquerading site. In one recent case, cyber-criminals obtained financial data from bank customers by setting up a web site with a name almost identical to the bank's name, prompting the Comptroller of the Currency to recommend safeguards that banks should adopt to prevent similar occurrences.[16] Now that such standards have been announced, the failure of a bank, or even another company, to adopt these or similar safeguards may leave a company unnecessarily vulnerable to claims by customers of, among other things, breach of contract and negligence.

Liability to Other Companies for Business Loss

Companies may also face liability exposure if a cyber-crime committed against them somehow causes business loss to another company. For example, companies could face contractual liability if a cyber-crime renders them unable to fulfill their contractual duties to another company, either because of lost data or temporary service stoppages.

Additionally, companies may find themselves the subject of multiple civil suits brought by a myriad of third parties if the company's computers are compromised as part of a directed denial of service ("DDOS") attack.[17] In such an attack, a hacker accesses the inadequately-secured computers of one company and uses them to send voluminous traffic (*e.g.*, e-mail) to another company's computers, thereby overloading the second company's systems. The affected company may then attempt to recover its business losses by bringing suit based on a theory of negligence against the company whose computers were used as instruments in the attack.[18]

Companies may also face liability exposure if a cyber-crime committed against them somehow causes business loss to another company.

Fortunately for a defendant company, plaintiff companies are burdened not only with causation problems (much like those discussed earlier in relation to customer claims) but also with demonstrating that the defendant owed the plaintiff-company a duty of care and/or that the plaintiff-company was a foreseeable victim of the defendant's negligence.[19] Nevertheless, although targeted companies in the end may prove successful in undermining claims for business loss, the costs of litigation and the risk to both reputation and public image may themselves be damaging enough to render a finding for the defendant little more than a hollow victory.

Other potentially cognizable claims for business loss include claims against a company whose computers were used to spread viruses or other malicious code as well as claims by companies to recover losses suffered from accepting seemingly good credit card numbers which, in fact, had been stolen from another company.

Liability to Shareholders for Network Breaches

The possibility of shareholder litigation is a risk that companies must also bear in mind. Any perceived failure to safeguard network resources—whether causing loss of confidential and/or proprietary data or disruption of services—could result in one or more shareholders bringing a derivative suit against company officers and directors for a breach of fiduciary duty. The greater the damage to a company's business, of course, the more likely it is that shareholders will bring such an action. A derivative suit would likely rest on a theory that the inadequate cyber-security system and

©2002 GLASSER LEGALWORKS

subsequent breach caused a decline in share value, either by causing direct economic loss to the company or based on the market's perception of risk resulting from the inadequately secured system. Even if such suits prove unsuccessful, the costs of litigation, corporate infighting and divisiveness, and negative publicity might be enough to bury an already struggling business.

Liability to Government Agencies for Failing to Comply with Regulations

Companies in certain industries also may be subject to regulatory actions for maintaining inadequate cyber-security measures. For example, many companies—including certain healthcare entities,[20] financial institutions,[21] and companies that collect online information from children[22]—are subject to privacy regulations enacted within the past five years that require them to protect certain types of online information.[23] Each set of regulations authorizes the governing agency to institute enforcement actions against companies that fail to comply with the mandated standards of care.[24]

The possibility of shareholder litigation is a risk that companies must also bear in mind.

In addition to privacy regulations, some industries are governed by reporting requirements. A financial institution that detects a "known or suspected" cyber-crime may be required to file a Suspicious Activity Report ("SAR"), regardless of whether the institution knows the identity of the perpetrator.[25] Failure to file an SAR can subject the institution to supervisory action, including the imposition of civil money penalties.[26]

Finally, certain companies, regardless of industry, may find themselves the target of regulatory actions if they fail to safeguard particular categories of non-private information, *e.g.*, materials readily available on a proprietary Internet site. Publicly-traded companies provide a prime example. These companies are required by the SEC to "take reasonable precautions to ensure the integrity and security of [publicly-provided] information, regardless of whether it is to be delivered through electronic means or paper."[27] A company that fails to do this and therefore fails to abide by SEC regulations could find itself facing action by either the SEC or actual purchasers or sellers of the company securities.[28]

Developing a Cyber-Security Plan to Mitigate Exposure

A key strategy for managing the legal risks associated with cyber-crime is to develop an effective cyber-security plan. Such a plan must go beyond the technical measures now emphasized by industry analysts. Although technical protections such as firewalls and intrusion detection systems are critical, they should be combined with non-technical safeguards to afford companies more complete protection against the various potential losses that could result from cyber-crime. Yet, all too often companies are not taking these steps. As the Deputy Chief of the Justice Department's Computer Crime and Intellectual Property Section recently observed: "the victims . . . have no response plan in place; they don't involve their lawyers, and all too often, they don't involve law enforcement."[29]

What follows is a list of considerations essential to mitigate potential legal exposure from cyber-crime. To the extent possible, these elements should be incorporated into a written cyber-security plan, which should be reviewed and updated at least annually. Developing and implementing such a plan not only encourages internal compliance, but also serves, in the event of legal action, as valuable evidence of a company's care to develop a complete cyber-security system.

Determine Cyber-Security Needs

Determining a company's precise cyber-security needs is a dynamic multi-step process in which company executives, managers, IT staff, and lawyers should be involved. First, companies should identify the cyber risks to which they are susceptible. To this end, a complete review of the network system and all potential architectural and technological vulnerabilities must be conducted. Second, companies should fully understand the applicable legal standards of care as well as any relevant regulatory standards. Third, companies should identify the costs associated with a network breach, including repair costs, business loss, and litigation expenses. Fourth, companies should assess the costs of adopting the various technical safeguards intended to plug identified system vulnerabilities.

Once companies complete these four steps, they must balance the attendant costs (including legal liability exposure) of a network security breach against the costs of adopting cyber-security safeguards. In order to perform this balancing test, companies must ensure that they have the expertise to select from among the range of applicable standards of care to which they might be subject and to evaluate whether the safeguards they intend to adopt actually comply with these standards.[30]

In determining standards of care, companies also must taken into account any applicable regulatory standards. This too requires considerable expertise. For example, certain health care organizations are required to adopt measures to protect patient health information and to detect and "mitigate" damages caused by computer breaches. Likewise, financial institutions are required to protect consumer data in a manner commensurate with "the size and complexity of the bank and the nature and scope of its activities."[31]

Assess Whether to Outsource

After a company has determined its precise cyber-security needs, the company then must decide whether it is capable of handling its own cyber-security needs or whether it must outsource them to a third party. For many smaller companies, particularly those that lack the resources

©2002 GLASSER LEGALWORKS

to hire in-house network security experts, outsourcing is a necessary option. Outsourcing, however, is not without risk, including loss of control over data, proprietary information, or other closely-held material.

For this reason, companies—both large and small—must not only exercise great care in selecting the contractor to whom security needs will be outsourced but also must ensure that the contractor, once hired, maintains an adequate level of security to meet the outsourcing company's cyber-security needs. To that end, companies should negotiate a contract that provides the outsourcing company with the practical security safeguards and legal liability protections that are in its interests while also giving the contractor incentive to perform at a high level.[32]

Adopt Technical Security Measures

Regardless of whether a company chooses to outsource network security, a comprehensive cyber-security plan should also include detailed descriptions of the technical safeguards to be adopted and the procedures for implementing those measures. Industry analysts regularly discuss the availability of various security technologies, and for this reason, these measures are not addressed in this article. Suffice it to say that common safeguards include such measures as maintaining firewalls to regulate incoming traffic, using encryption software to protect the transmission of data, and monitoring and filtering of both incoming and outgoing traffic to prevent the company's computers from being used in DDOS attacks.

Monitor for New System Vulnerabilities

Technical safeguards are only adequate when they are combined with protocols for both monitoring their ongoing effectiveness and plugging identified holes. For example, computer experts can monitor current industry trends and developments in order to identify further improvements that should be made to a company's technical safeguards. Today, a significant breadth of resources exists for upgrading technical safeguards including web sites operated by government centers (such as the National InfraStructure Protection Center), private organizations (such as the Computer Security Institute), vendors (such as Microsoft), and peer networking companies. Incorporating provisions detailing the use to be made of these resources into a cyber-security plan is critical because failure to adopt even basic safeguards like installing patches against known problems can open companies to substantial risk of liability.[33]

In addition, depending on the nature and size of the company, the cyber-security plan may include procedures for periodically testing the security of a company's computer system. Computer experts, whether in-house or retained, may test the effectiveness of a company's security measures by attempting to infiltrate its network system. If holes in the system are identified, these same experts can take the necessary steps to reconfigure the out-of-date firewall or tweak the lagging intrusion detection system.

Manage Employee Use

Many cyber-crimes are perpetrated by current or former employees.[34] To limit this risk, companies should adopt appropriate policies and procedures related to the hiring, training, oversight, and termination of employees. Hiring procedures should include proper background checks and a requirement that certain employees sign confidentiality agreements. Employee training should include education on company procedures and methods for promoting cyber-security and, for certain industries, compliance with controlling security-related regulations.

Oversight should include ensuring that only certain employees have access to confidential information, monitoring computer activity for wrongdoing, ensuring that employees follow proper security measures (such as maintaining confidentiality of and regularly changing passwords), and providing employees with reminders of their security obligations (such as through the use of policy banners at the point of system log-in). Termination procedures should, among other things, ensure that former employees' passwords are immediately disabled upon departure and that these employees are otherwise blocked from future access to the company's computer systems.

Use Contracts to Limit Liability

Where possible, contracts with customers and business partners should be negotiated to contain provisions that serve to limit a company's liability for cyber-crimes directed against its own network as well as cyber-crimes impacting company data residing on the network of a contractor. One popular provision limits a company's liability for stolen data to instances where the company *recklessly* stored the information on its own network and/or *recklessly* shared the data with a contractor who then failed to protect it.

Develop an Immediate Response

A key to developing an effective cyber-security plan is determining ahead of time what to do if a cyber attack occurs. Such a protocol should take into account basic elements, such as how to identify a cyber attack,[35] steps to be taken to contain the attack, and methods for preserving evidence of the attack. The protocol also should include guidelines on maintaining records of the breach for internal purposes *(e.g.*, to plug the exposed vulnerability) as well as for external purposes (*e.g.*, to provide to law enforcement if requested). To do this, companies must possess the technical means to log activity and to take basic steps to preserve evidence, as even the simple act of turning on a computer after a hack can destroy valuable evidence.

Develop a Plan to Report Hacks to Potentially Affected Parties

Companies also should have an established protocol for identifying potentially affected parties, including customers, business partners, and investors. The protocol should include a list of considerations (*e.g.*, regulatory requirements, contractual obligations, consequent harm to party if

©2002 GLASSER LEGALWORKS

not reported) to guide the decision of *whether* and *when* to notify affected parties. Although proper notification can avoid or limit liability while at the same time maintaining goodwill, untimely or otherwise inappropriate notification can expose the company to further risk of liability.

Develop a Plan to Notify Law Enforcement

Similarly, a comprehensive cyber-security plan should contain protocols for determining *whether* and *when* to notify law enforcement. In making the decision whether or not to notify law enforcement, companies must balance competing concerns. Some companies may be reluctant to notify law enforcement of every network breach because of perceived publicity concerns, risk of liability, and the potential for delays and costs should law enforcement initiate an investigation.[36] However, some of these concerns may be overstated[37] and, in some instances, may fail to take into consideration the benefits of notifying law enforcement, including preventing further attacks[38] and reducing potential tort or contract liability.

If the decision is made to notify law enforcement, then companies must know how to go about reporting the hack. For this reason, a cyber-security plan should include detailed information on the appropriate law enforcement agency to contact, how to work with that agency to limit any damaging publicity, and how to cooperate with the agency in a way that protects the company's interests, including the privacy interests of third parties.

Finally, a complete cyber-security plan should contain guidance on identifying when regulatory reporting requirements are triggered by a hack attack or other cyber-crime. Failure to comply with such reporting requirements can lead to the imposition of civil money penalties as well as unwanted regulatory oversight and negative publicity.

Assess Rights Against Other Parties

Knowing one's obligations to third parties and government agencies is only one piece of the cyber-security puzzle. Companies must also be aware of their legal rights. This includes knowing the avenues available for obtaining information about the hack from other companies, such as Internet service providers, and knowing whether and in what fora to seek recovery of business and other cyber-crime-related losses from partners, vendors, and third parties.

Secure Insurance Coverage

Far too many companies fail to evaluate whether their existing insurance policies cover most, if not all, of their cyber-crime-related exposures.[39] Rather than simply renewing existing, possibly outdated, policies, prudent executives, in close consultation with legal counsel, should evaluate their company's insurance needs and obtain policies that address those risks. In particular, companies should examine carefully the coverage provided by traditional policies (such as commercial general liability), and consider the benefits, if any, of specialty products, designed by insurance companies to cover risks associated with cyber-crime. The goal should be to create a seamless blanket of policies providing coverage for foreseeable cyber-crime risks.

Contribute to Legislation and Regulations

Given mounting concerns about computer security and individual privacy, further legislation and regulation in the area of cyber-crime is all but guaranteed. One issue gaining increased attention in recent months is the extent to which the government may seek to promote participation by companies in cyber-security enforcement and prophylactic activities, or, conversely, seek to impose liability on companies for cyber-security risks. For example, Congress introduced legislation last year that would facilitate a company's sharing of information about cyber-crimes and would protect certain information provided to the government from disclosure under the Freedom of Information Act.[40] Companies should consider whether, and if so how, to participate in the public debate on this key issue.

Conclusion

The increasing use of computers and the Internet poses new security risks for companies. Most companies already maintain technical safeguards, but few companies appear to have adopted the kind of complete cyber-security program necessary to safeguard not only against direct loss, but also against substantial legal exposure. Only by adopting these measures will companies be able more effectively to manage and limit their risk of cyber-crime loss. ●

Notes

1 Most computer hacking that causes injury is penalized under one or more federal or state statutes. *See, e.g.*, 18 U.S.C. § 1030.

2 *See* Michael Barbaro, *Internet Attacks On Companies Up 28 Percent, Report Says*, WASH. POST, July 8, 2002, at E5.

3 To learn more about the Computer Security Institute (a San Francisco-based international association of computer security professionals) or its survey, visit the Computer Security Institute Website at <http://www.gocsi.com>.

4 *See* Computer Security Institute, *Cybercrime bleeds U.S. corporations, survey shows* (April 7, 2002), *available at* <http://www.gocsi.com/press/20020407.htm> (survey by joint FBI/private venture).

5 *See id.* The respondents who were capable of quantifying their losses said they lost close to $115.8 million due to financial fraud and $170.8 million from the theft of proprietary information. *See id.*

6 David A. Vise & Daniel Eggen, *FBI Warns of Cyber-Attack Threat: U.S. 'Very Concerned' About Vulnerability of Infrastructure*, WASH. POST, Mar. 21, 2001, at A16.

7 *See* Brian Fonseca, *IT Security Under the Gun*, INFOWORLD, Mar. 12, 2001, *available at* http://www.itworld.com/Sec/3832/itwnws010312security/.

8 *See* Barton Gellman, *Cyber-Attacks by Al Qaeda Feared*, WASH. POST, June 27, 2002, at A1 ("Unsettling signs of al Qaeda's aims and skills in cyberspace have led some government experts to conclude that terrorists are at the threshold of using the Internet as a direct instrument of bloodshed.").

9 *See* Michael James, *Small Thefts, Big Trouble*, BALTIMORE SUN, Jan. 22, 2001, at C1 (reporting consumer class action brought against online companies for failing to secure consumers' credit card data adequately); *Nike sued for hacking costs*, NEWSWIRE (Mar. 28, 2001)

©2002 GLASSER LEGALWORKS

(reporting threatened suit against Nike for loss of business resulting from Nike's alleged failure to secure computers).

10 A Baltimore attorney has reportedly filed a class action on these grounds. *See* Michael James, *Small Thefts, Big Trouble*, BALTIMORE SUN, Jan. 22, 2001, at C1.

11 For example, *Time* magazine recently warned individuals of the dangers they face from cyber-crime in a cover article, including by recounting various incidents where customer data was stolen from companies. *See Internet Insecurity*, TIME, July 2, 2001, at 44.

12 *See, e.g.*, Ariana Eunjung Cha, *Hackers Steal Subscriber Data from AOL Network*, WASH. POST, June 17, 2000, at E1 (describing breach in security of AOL's network that resulted in theft of consumer names, addresses, and credit card numbers).

13 *See, e.g.*, Dan B. Dobbs, *The Law of Torts* 269 (2001) (listing the elements of a negligence claim).

14 *See, e.g.*, *Restatement (Second) of Torts* § 448 ("The act of a third person in committing an intentional tort or crime is a superseding cause of harm to another resulting therefrom, although the actor's negligent conduct created a situation which afforded an opportunity to the third person to commit such a tort or crime, unless the actor at the time of his negligent conduct realized or should have realized the likelihood that such a situation might be created, and that a third person might avail himself of the opportunity to commit such a tort or crime").

15 For example, a company might share credit card numbers with a clearing house from which the numbers were stolen. The customer could argue that the company failed to ensure that the clearing house had adequate security before turning over the numbers.

16 *See* Comptroller of the Currency, Alert 2000-9: Protecting Internet Addresses of National Banks (July 19, 2000).

17 In February 2000, a series of denial-of-service attacks launched against businesses such as Amazon.com, Yahoo, E*Trade, and eBay resulted in estimated losses of $1.2 billion for the affected companies. The $1.2 billion loss figure did not include costs associated with liability exposure. *See* Denise Pappalardo, *Avoiding future denial-of-service attacks*, NETWORK WORLD FUSION, Feb. 23, 2000.

18 A Scottish company threatened to bring an analogous claim against Nike in the United States, after Nike's computer traffic was routed through the company's servers by a hacker who was directing the traffic to an anti-Nike site. The company actually sued Nike in Scottish court for the costs of rerouting the traffic back to Nike. *See Nike sued for hacking costs*, NEWSWIRE, Mar. 28, 2001.

19 *Cf. Restatement (Second) of Torts* § 302B ("An act or an omission may be negligent if the actor realizes or should realize that it involves an unreasonable risk of harm to another through the conduct of the other or a third person which is intended to cause harm, even though such conduct is criminal"). The plaintiff would also have to rebut the obvious comparative negligence defense the defendant could raise based on the plaintiff's own cyber-security system.

20 *See* 45 C.F.R. § 164.530(c)(1), enacted pursuant to 42 U.S.C. § 1320d-2 (Health Insurance Portability and Accountability Act of 1996).

21 *See* 12 C.F.R. part 30, appendix B § II.A (regulations implementing the Gramm-Leach-Bliley Act).

22 *See* 15 U.S.C. § 6502(b)(1)(D) (Children's Online Privacy Protection Act); 16 C.F.R. § 312.8.

23 *See* 64 Fed. Reg. 59888 (Nov. 3, 1999) (FTC security recommendations for companies governed by the Children's Online Privacy Protection Act); 45 C.F.R. § 164.530(c)(1) (requiring covered health care entities to adopt "appropriate administrative technical, and physical safeguards to protect the privacy of protected health information" and to adopt means of mitigating damages from the disclosure of protected information); 12 C.F.R. part 30, appendix B § II.A (requiring financial institutions to train staff on the institution's security measures, regularly test these measures, and employ technical protections such as encryption and access restrictions).

24 *See* 16 C.F.R. § 312.9; 42 U.S.C. § 1320d-5 (allowing $100 fine for each violation of health care regulations, up to $25,000 per year for same violation); 15 U.S.C. § 6805 (allowing enforcement of Gramm-Bliley-Leach Act under banking laws).

25 *See* 12 C.F.R. § 208.62; *id.* § 21.11; *id.* § 563.180; *id.* § 748.1. Lack of knowledge of the identity of the hacker only gives the institution an additional 30 days to file the report.

26 Although implausible, it is even possible for a company to face criminal liability for concealing a cyber-crime, as actively concealing a felony can be a violation of the federal misprision statute. *See* 18 U.S.C. § 4. Thus, in 1996, the government charged Daiwa Bank, Ltd. with misprision for hiding a rogue trader's large losses through falsification of records and other means. *See* Matthew E. Beck & Matthew E. O'Brien, *Corporate Criminal Liability*, 37 AM. CRIM. L. REV. 261, 272-73 (2000). Daiwa settled the case for a record $340 million.

27 Use of Electronic Media for Delivery Purposes, S.E.C. Docket 1091, File No. S7-31-95, n.22 (Oct. 6, 1995).

28 One commentator has suggested that such claims could be brought under Rule 10b-5. *See* Robert A. Prentice, *The Future of Corporate Disclosure: The Internet, Securities Fraud, and Rule 10b-5*, 47 EMORY L.J. 1, 47-48 (1998) ("This is a particularly plausible theory because of the SEC's explicit position that companies communicating electronically with shareholders and potential investors must take 'reasonable precautions' to ensure the 'integrity and security' of information however it is delivered."). The most significant impediment to bringing such a claim is the *scienter* requirement. Conceivably, however, a plaintiff could show the necessary *scienter* on the part of the company by relying on one of the many recklessness standards endorsed by different courts, *see, e.g.*, *Greebel v. FTP Software, Inc.*, 194 F.3d 185, 198-201 (1st Cir. 1999), and arguing that the company was reckless because it maintained inadequate security or failed to monitor its web site to detect and correct changes promptly.

29 *Say It Again, Uncle Sam: Federal Cyber-Police Repeat Claims That Net Security Is Too Lax*, SECURITY & ENCRYPTION, Apr. 18, 2001, at 602.

30 These standards might be based on those proposed by a government/private interest venture like the National Infrastructure Protection Center; those advocated by private industry groups, such as the Internet Security Alliance, which was jointly formed by Carnegie Mellon University's Software Engineering Institute and the trade group Electronic Industries Alliance, *see* Charles Bogino, *New Industry Alliance Hopes to Halt Attacks on Networks, Seeks Increase in Membership*, DAILY REPORT FOR EXECUTIVES, Apr. 20, 2001, *available at* <http://pubs.bna.com/ip/BNA/der.nsf/id/a0a4d0v0v5>; standards urged by industry commentators, *see, e.g.*, Robert A. Bourque & Blake A. Bell, *Protecting Customers' Private Data from Institutional Identity Thieves*, N.Y.L.J., Sept. 7, 2000; David L. Gripman, Comment, *The Doors Are Locked But the Thieves and Vandals Are Still Getting In*, 16 J. MARSHALL J. COMPUTER & INFO. L. 167, 184-91 (1997); or some other type of standards.

31 12 C.F.R. part 30, appendix B § II.A.

32 For examples of provisions to be added to outsourcing contracts, see the section on Outsourcing contained in "Cybersecurity: Risk and Liability in the New Information Environment," authored by D. Jean Veta, et al., which will appear in the forthcoming treatise *Information Technology and Electronic Commerce: Law and Practice* (Aspen Law & Bus., forthcoming 2002).

33 *See* Robert Lemos, *Virus patches aren't being applied*, ZDNET NEWS, Jan. 24, 2001, (citing estimate that failure to patch led to 99% of web site defacements last year).

34 *See, e.g.*, *Law enforcement agencies ask for tougher computer crime laws*, *available at* <http://www.siliconvalley.com/docs/news/tech/069810.htm> (reporting congressional testimony about former bank employee who recently shut down its entire network).

35 *See* Peter Piazza, *No Relief from Hack Attacks*, SECURITY MANAGEMENT, Jan. 1, 2001 (noting estimates that by 2003, half of all small- and medium-sized businesses will be hacked, with only 60% of these businesses being able to tell that they were hacked).

36 These concerns have apparently led companies to underreport cyber-crimes to law enforcement. *See Financial losses due to internet intrusions, trade secret theft and other cyber crimes soar* (Apr. 7, 2002), *available at*

©2002 GLASSER LEGALWORKS

<http://www.gocsi.com/press/20020407.htm> (reporting that only 34% of survey respondents reported computer intrusions to law enforcement).

37 *See, e.g.*, *Say It Again, Uncle Sam: Federal Cyber-Police Repeat Claims That Net Security Is Too Lax*, SECURITY & ENCRYPTION, Apr. 18, 2001, 602-03 (noting recent statement by the head of the National Infrastructure Protection Center that the government has shown increasing sensitivity to companies' publicity concerns).

38 Bloomberg LP demonstrated the value of working with law enforcement when it lured an extortionate hacker to a meeting where he could be arrested, thereby removing the threat posed by the hacker and garnering favorable publicity. *See* United States Attorney, Southern District of New York, *Three Kazak Men Arrested in London for Hacking into Bloomberg L.P.'s Computer System* (Aug. 14, 2000), *available at* <http://www.usdoj.gov/criminal/cybercrime/bloomberg.htm>.

39 Legal exposure varies with a company's Internet presence. For example, the exposure of a company that operates a web site may vary depending on such factors as whether the site provides content only, whether the content is provided by third parties, whether the site provides advice, whether the site gathers personal information from visitors, or whether other businesses rely on the site for their own revenue.

40 *See* Matthew Morrissey, *Davis, Moran Introduce Bill Allowing Firms to Share Cyber-Attack Information*, DAILY REPORT FOR EXECUTIVES, July 11, 2001, *available at* <http://pubs.bna.com/ip/BNA/der.nsf/id/a0a4k3f0a5>.