STEPTOE & JOHNSON LLP

ATTORNEYS AT LAW

1330 Connecticut Avenue, NW
Washington, D.C. 20036-1795

Telephone 202.429.3000
Facsimile 202.429.3902
http://www.steptoe.com

A PATCH IN TIME SAVES NINE: LIABILITY RISKS FOR UNPATCHED SOFTWARE

Stewart Baker
Steptoe & Johnson LLP
Telephone: 202.429.6413
Fax: 202.261.9825
Email: sbaker@steptoe.com

Maury Shenk
Steptoe & Johnson
Telephone: +44.20.7367.8092
Fax: +44.20.7367.8001
Email: mshenk@steptoe.com

October 2003

In the first eight months of 2003, the international information technology community faced three serious Internet worm attacks – the SQLSlammer worm in January, the Blaster worm in early August, and the Sobig worm in late August. The SQLSlammer and Blaster outbreaks were largely preventable – as long as network operators moved quickly to install security patches.[1] SQLSlammer exploited a vulnerability in Microsoft SQL Server 2000 that was publicly identified in July 2002, and Blaster exploited a vulnerability of Microsoft Windows that was publicly identified in mid-July 2003. In each case, Microsoft released a security patch at the same time that the vulnerability was publicly identified. These security patches could have significantly moderated the effects of the attacks, if they had been promptly applied by users. But the lead time grew significantly shorter in the course of the year. IT managers, who had months to respond to the security flaw exploited by SQLSlammer, had only a couple of weeks to patch the hole that Blaster used. Even so, most of the damage done by these worms could have been avoided by a program of promptly installing patches.

Security experts have been recommending such programs for years, invoking the old saw that "a stitch in time saves nine". It is largely undisputed that the effort and expense of installing security patches is generally less than the effort and expense of recovering from attacks that exploit unpatched vulnerabilities. Yet malware[2] continues to exploit known, patchable vulnerabilities – and to cause growing damage. This article considers whether public unhappiness at the effects of such exploits will spill over into the legal system – that is, whether companies face legal liability if they do not apply security patches promptly, or if they run

---

[1] The Sobig worm propagates through malicious code in e-mail attachments, so only became strictly preventable after it appeared, when virus software vendors released updates to block the worm.

[2] "Malware" refers to viruses, worms, Trojan horses and other software that is specifically designed to attack computer systems.

insecure software for which patches are not available. For the reasons we set out below, we believe that the risks of such liability are already significant, and are likely to increase over time.

I. The Patch Process

Security vulnerabilities are in computer operating systems and other software, despite the best efforts and intentions of programmers. Two leading computer security experts recently wrote:

> In all our years of working in this field, we have yet to see an entire system that is secure. That's right. Every system we have analyzed has been broken in one way or another.[3]

Both the good guys (computer security professionals) and the bad guys (hackers) are constantly looking for new security vulnerabilities. A few years ago, there was an ongoing debate regarding whether and when vulnerabilities identified by the good guys should be publicly disclosed – since the significant benefits of public disclosure (*i.e.*, allowing users to fix the vulnerability) are partially counterbalanced by the fact that more bad guys are made aware of the vulnerability (in reality any benefit of secrecy is fairly limited, since news of vulnerabilities typically travels quickly in the hacker community). The current consensus is that vulnerabilities should be publicly disclosed after the software manufacturer is notified and given time to rapidly develop a patch.

The most respected source of information on security vulnerabilities is the CERT Coordination Center ("CERT"[4], http://www.cert.org), which is located at a federally-funded research institution at Carnegie Mellon University in Pennsylvania. Similar information is available from a variety of other sources, including the U.S. Department of Homeland Security

---

[3] Niels Ferguson & Bruce Schneier, *Practical Cryptography*, p. 1 (2003)

[4] CERT was originally the Computer Emergency Response Team, but now uses only the acronym.

("DHS"), which maintains information on security vulnerabilities through its Information Analysis and Infrastructure Protection Directorate[5] and has recently announced a collaboration with CERT to create the U.S. Computer Emergency Response Team ("US-CERT").[6] Typically, a security vulnerability is publicly identified in a CERT "advisory" at about the same time that the manufacturer addresses a patch to correct the vulnerability. For the vulnerability exploited by SQLSlammer, the CERT advisory and Microsoft patch were released on the same day; and for the vulnerability exploited by Blaster, the Microsoft patch was released one day before the CERT advisory.

Once a security vulnerability has been identified by CERT (or otherwise) and a patch made available, the patch must be installed by users. This is not necessarily a straightforward process. Even for large companies and organizations that have personnel tasked with implementing patches, problems include ensuring that patches (1) are deployed to every affected computer and (2) are compatible with the organization's existing computing environment. The first issue is a difficult one in organizations with many thousands of computers, and is particularly serious given that a single unpatched computer can threaten the security of a network. On the second issue, most network administrators have tales to tell about patches that fixed a hole but broke the network, or at least certain applications. Even Microsoft recognizes that there is some risk of disruption when a user installs one of its patches:

> **Rollback considerations.** Can a release by uninstalled? Are necessary provisions in place in the event a computer stops responding after a patch is deployed? Are the proper data backup and restore procedures taking place? Understanding the requirements for returning computers to their original state in

---

[5] *See* http://www.dhs.gov/dhspublic/interapp/editorial/editorial_0335.xml.

[6] *See* "Secretary Ridge Announces the Creation of New Computer Emergency Response Center for Cyber Security," DHS press release (Sept. 15, 2003).

> the unlikely event that a deployment adversely affects your environment is an important aspect of release management.[7]

Small organizations and individuals face the additional problem of identifying when patches are needed. For recent versions of Windows, Microsoft automates this process with the Windows Update feature that checks online for patches, but this feature does not eliminate the compatibility issue noted above, and does not help for security vulnerabilities of the majority of software products for which no such update service is available – *e.g.*, various other Microsoft products, and Cisco Systems devices running the IOS operating system (which CERT recently identified as being vulnerable to denial-of-service attacks).

A related and even more difficult dilemma exists for companies that continue to use software that has known security vulnerabilities, but which the manufacturer no longer supports with patches – for example, this is the case for Windows 98. To eliminate security risks, such companies may have little choice but to upgrade to new software, which involves both greater expense and greater implementation difficulties than application of a patch.

Available evidence suggests that current patching practices are, well, "patchy". In recent Congressional hearings, the senior technologist of security company Qualys provided some observations based upon the company's database of network vulnerabilities, including the following:

> The half-life of critical vulnerabilities is 30 days and doubles with lowering degrees of severity. In other words, for even the most dangerous vulnerabilities, it still takes organizations 30 days to patch 50% of the vulnerable systems, leaving them exposed for a significant period of time. . . .

---

[7] *The Microsoft Guide to Security Patch Management*, p. 113, available at http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/topics/patch/secpatch/Default.asp (2003).

> The lifespan of some vulnerabilities is unlimited. Old risks recur partly due to new deployment of PCs and servers with faulty unpatched software.[8]

Whether patching practices improve is likely to depend heavily on the severity of consequences from failure to patch, including consequences resulting from legal liability.

II. Legal Bases of Liability

Liability for failure to apply security patches could exist either pursuant to statute and regulation, or under common law contract and tort principles. We consider likely claims from both of these sources of law.

A. Statute and Regulation

Congress has enacted two laws that apply detailed computer security requirements to specific sectors: the Health Insurance Portability and Accountability Act ("HIPAA"),[9] which applies to the health sector; and the Gramm-Leach-Bliley Act ("GLBA"),[10] which applies to the financial sector. Both statutes include broad obligations to protect the security of the information, and direct federal regulators to adopt regulations to implement those provisions.

Pursuant to GLBA, the four U.S. banking regulators (the Office of the Comptroller of the Currency, the Office of Thrift Supervision, the Board of Governors of the Federal Reserve System, and the Federal Deposit Insurance Corporation) in 2001 adopted interagency guidelines that require any regulated financial institution, among other things, to:

> Protect against any anticipated threats or hazards to the security or integrity of [customer] information; …

---

[8] *Hearing on Worm and Virus Defense: How Can We Protect the Nation's Computers From These Threats? Before the House Subcomm. on Technology, Information Policy, Intergovernmental Relations and the Census*, 108th Cong. (2003) (statement of Gerhard Eschelbeck, Chief Technology Officer and V.P. of Engineering, Qualys, Inc.).

[9] Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191 (1996).

[10] Gramm-Leach-Bliley Act, Pub. L. No. 106-102 (1999).

> Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer[; and] …
>
> Design its information security program to control the identified risks, commensurate with the sensitivity or the information as well as the complexity and scope of the bank's activities.[11]

Likewise, pursuant to HIPAA, the U.S. Department of Health and Human Services in 2003 adopted regulations that require health-care providers, among other things, to:

> Protect against any reasonably anticipated threats or hazards to the security of [health] information[;] …
>
> Implement … [p]rocedures for guarding against, detecting, and reporting malicious software[; and] …
>
> Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights … .[12]

These regulatory obligations appear to require the affected entities to implement at least some sort of security patch procedures.

Both HIPAA and GLBA place responsibility for enforcement of these regulations in the hands of federal regulators, and do not create any right of private individuals to sue based on the regulations (known in legal terms as a "*private right of action*"). However, the regulations provide persuasive evidence of proper security practices, at least in the health care and banking sectors. Such evidence could be of significant weight in private actions under common law, as discussed in section II.B below.

GLBA and HIPPA are not the last security-related initiatives likely to emerge from legislatures and regulatory bodies. Their continued appetite for new rules in the field is

---

[11] Interagency Guidelines Establishing Standards For Safeguarding Customer Information, §§ II.B.2, II.B.3, III.C.1, 66 Fed. Reg. 8615 (Feb. 1, 2001).

[12] 45 C.F.R. §§ 164.306(a)(2), 164.308(a)(5)(ii)(B), 164.312(a)(1).

demonstrated by the popularity of requiring companies to notify consumers about security breaches. In California, Senate Bill No. 1386 ("SB 1386") took effect in July 2003, requiring any business or other organization to disclose any security breach that compromises unencrypted personal information of California residents (and most large U.S. businesses serve California residents).[13] Significantly, SB 1386 includes a private right of action against organizations that fail to comply with this disclosure obligation. Senator Diane Feinstein of California has proposed federal legislation which would have the same effect on a nationwide basis (without a private right of action),[14] but this legislation so far appears fairly unlikely to make progress in Congress. And in August 2003, the four federal banking regulators exercised their authority under GLBA to issue "guidance" indicating that part of the response by financial institutions to a security breach should be to notify federal regulators, law enforcement and customers.[15] This disclosure guidance as practical matter is binding on U.S. financial institutions. While these disclosure obligations do not directly affect liability for security failures, they will encourage more security-related litigation by telling the victims of security failures exactly who is to blame. In addition, it is only reasonable to expect that lawyers suing over a failure to provide notice of a security breach will also throw in a few counts alleging liability for the underlying breach itself.

So far, no generally-applicable federal or state legislation imposes cross-sectoral computer security requirements. Nor does any enactment couple general computer security obligations with a right of private parties to sue for damages (in contrast to the more limited right to sue for failure to notify under California's SB 1386). But cybersecurity has been getting a lot

---

[13] *See* Cal. Civil Code §§ 1798.29, 1798.82, 1798.84.

[14] S. 1350, 108th Cong. (2003).

[15] Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, 68 Fed. Reg. 47,954 (Aug. 12, 2003).

of recent attention in Congress, and such legislation is not beyond the realm of possibility. Cybersecurity hearings were held in June 2003 before the House Subcommittee on Cybersecurity, Science, and Research and Development and in September 2003 before the Technology Subcommittee of the House Government Reform Committee. There is no evidence that the chairmen of these subcommittees (Congressmen William "Mac" Thornberry (R-CA) and Adam Putnam (R-FL), respectively) would support legislation giving consumers a right to sue for damages for security breaches – rather, they have both focused on market-based incentives like tax breaks to promote security. But they have made noises that something needs to be done. Rep. Thornberry said in August 2003:

> You don't want to be too quick on the draw with new mandates. But you can't be too hesitant to pull the trigger when there are concerns.[16]

Some of those testifying before their committees have been much more definitive. Leading computer security expert Bruce Schneier recommended:

> Expose computer hardware, software, and networks to liabilities. … The major reason companies don't worry about the externalities of their security decisions – the effects of their insecure products and networks on others – is that there is no real liability for their actions. Liability will immediately change the cost/benefit equation for companies, because they will have to bear financial responsibility for ancillary risks borne by others as a result of their actions. With liabilities firmly in place, the best interests of software vendors, and the best interests of their shareholders, will be served by them spending the time and money necessary to secure their networks.[17]

Ideas like this may ultimately gain some legislative traction, particularly in light of the increased attention that has been given to security issues since September 11, 2001.

---

[16] "Congressman: Businesses Must Help Protect Net," *IDG News Service* (Aug. 15, 2003).

[17] *Hearing on Overview of the Cyber Problem – A Nation Dependent and Dealing with Risk Before the House Subcomm. on Cybersecurity, Science, and Research and Development*, 108th Cong. (2003) (statement of Bruce Schneier, Founder and Chief Technical Officer, Counterpane Internet Security, Inc.). Schneier was quoted making similar points in a recent article in the *Financial Times*. *See* Richard Waters, "When will they ever stop bugging us?," *Financial Times* (Sept. 16, 2003).

In the specific area of security patches, Congressman Cliff Stearns of Florida in 2003 introduced privacy legislation that would, among other things, require organizations to apply patches in response to security advisories issued by the Department of Homeland Security ("DHS").[18] Although this proposed legislation explicitly states that it does not create a private right of action, companies already face significant liability risks for failure to implement available patches in response to advisories from entities like CERT and DHS.

Beyond such existing and possible legislation specifically related to security, legislation in other areas may also create risks for entities that use unpatched or outdated operating systems. In the wake of the Enron and WorldCom scandals, the Sarbanes-Oxley Act[19] introduced a variety of new governance requirements for publicly-traded companies. In particular, Section 404 of the Act requires company management to certify that effective internal controls for financial reporting are in place, and to disclose control deficiencies that could affect financial performance. The Securities and Exchange Commission ("SEC") rules implementing Section 404 define "internal control over financial reporting" to include:

> those policies and procedures that … (3) Provide reasonable assurance regarding prevention or timely detection of unauthorized acquisition, use or disposition of the registrant's assets that could have a material effect on the financial statements.[20]

It appears that the SEC would interpret this obligation as extending to controls on computer security, at least for those companies for which a security breach could have a material effect on their business. Indeed, in a recent paper the Institute of Internal Auditors has linked the

---

[18] H.R. 1636, § 105, 108th Cong. (2003).

[19] Pub. L. No. 107-204 (2002).

[20] Management's Report on Internal Control Over Financial Reporting and Certification of Disclosure in Exchange Act Periodic Reports, 68 Fed. Reg. 36,636, 36,640 (June 18, 2003).

obligations under the Sarbanes-Oxley Act to a variety of specific recommended security practices, including "Upgrade PC operating systems and other software to stay current with security patches and to ensure continuous vendor support for all software in use."[21]

Although our focus in this article is on U.S. law,[22] U.S. companies (particularly multinationals) cannot ignore the security concerns that arise under the European Union ("EU") Data Protection Directive,[23] and similar laws in other countries. The Data Protection Directive regulates "data controllers" that process personal data, and specifically requires implementation of security controls:

> Member States shall provide that the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing. Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.[24]

Although the Directive applies directly only in the EU, it also restricts transfers of data on EU-resident individuals to non-EU countries. The U.S. Department of Commerce and the European Commission in 2000 reached a Safe Harbor Agreement that sets out principles that U.S. companies can agree to follow in order to be permitted to receive data from the EU in

---

[21] *See, e.g.,* Mark Salamasick & Charles LeGrand, "Managing Desktop Security in an Insecure Environment," Institute of Internal Auditors paper (2003).

[22] Liability issues like those discussed in this article are likely to arise under the laws of many countries.

[23] Directive 95/46/EC of the European Parliament and Council, Art. 25 (1995).

[24] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Article 17(1).

compliance with the Directive; and many U.S. companies have agreed to follow these principles.[25] One of the Safe Harbor principles, entitled "Security", provides:

> Organizations creating, maintaining, using or disseminating personal information must take reasonable precautions to protect it from loss, misuse and unauthorized access, disclosure, alteration and destruction.[26]

Other countries have adopted cross-sectoral privacy laws along the lines of the EU Data Protection Directive, such as Canada's Personal Information Protection and Electronic Documents Act ("PIPEDA").[27]

For companies that are subject to the Sarbanes-Oxley Act, the EU Data Protection Directive (including via the Safe Harbor), and similar foreign legislation, these obligations increase the risks associated with unpatched software.

B. Common Law

In fact, courts don't need a special statute to hold companies liable for security breaches. There are two general-purpose common-law claims that could result in liability for failure to apply security patches – breach of contract (where the company has made explicit commitments regarding computer security) and negligence (even where it has not made such commitments).[28] Claims for intentional harm to customers or others – in legal terms, "intentional torts" – are also a possibility, but a remote one. Such claims are more difficult to prove, except perhaps in the

---

[25] *See* http://www.export.gov/safeharbor for information on the Safe Harbor Agreement and the companies that have joined it.

[26] U.S. Department of Commerce, Safe Harbor Privacy Principles, available at http://www.export.gov/safeharbor/SHPRINCIPLESFINAL.htm (2000).

[27] S.C. 2000, c.5 (Can.).

[28] One of the authors has previously written at greater length about breach of contract and negligence actions involving information security. *See* Stewart Baker & Melanie Schneck, "The Legal Significance of Information Assurance Standards," *The Executive's Desk Book on Corporate Risks and Response for Homeland Security* (National Legal Center for the Public Interest, 2003).

area of misrepresentation (which has been the basis of actions by the U.S. Federal Trade Commission that are discussed in section III below).

Breach of Contract. With respect to breach of contract, companies could face claims for failure meet express contractual obligations requiring compliance with internal or industry computer security standards, or standards pursuant to law or regulation. A company could also incur liability for failure to comply with implied contractual terms. Significantly, courts often imply obligations under applicable law into contracts,[29] and a failure to comply with statutory duties can be grounds for a breach of contract lawsuit.[30] However, there are limits to this principle: the U.S. Supreme Court has fairly recently stated that laws generally are implied into private contracts only when those laws affect the validity, construction, and enforcement of contracts.[31] That is, it appears most likely that statutory computer security obligations would be implied into contracts that include significant commitments regarding computer security, and less likely where security is an ancillary aspect of the contract. Thus, to the extent that statutory security obligations like those under HIPAA and GLBA (or possibly the Sarbanes-Oxley Act) are clearly applicable to the activities covered by a contract, a court could imply a private contractual requirement to comply with these obligations. Such implied contractual obligations could substantially lessen the comfort that companies might otherwise draw from the fact that these statutes do not provide a private right of action.

---

[29] *See, e.g., Armor Packing Co. v. United States*, 28 S. Ct. 428, 436 (1908) (the statute, being within the constitutional power of Congress, and being in force when the contract was made, is read into the contract and becomes a part of it).

[30] *See, e.g.*, *Selcke v. New England Ins. Co.*, 995 F.2d 688, 689 (7th Cir. 1993).

[31] *General Motors Corp. v. Romein*, 112 S. Ct. 1105, 1111-12 (1992).

Negligence. Contract law does not apply in the absence of an agreement (and therefore usually provides no remedy for damage to third parties) or where an agreement does not expressly or impliedly impose computer security obligations. In these circumstances, however, liability for negligence remains a risk. Negligence liability depends upon whether the a party who is sued has breached a "duty of care" to the party bringing the suit. In assessing whether a party has a duty of care, standards – *i.e.*, statutory and regulatory standards, as well as industry and corporate standards – play a much more significant role than in a contract case. Again, even without a private right of action, the requirements of GLBA and HIPPA could be read as creating a duty of care on the part of the financial or health care industries.

If the courts find that companies handling data or running networks do owe a duty of care to their customers, a question remains: What obligations does that impose on the companies? That will depend on several factors that have been identified by the courts in other negligence cases. First, the amount of caution required increases with the likelihood of injury. Second, a company's duty to protect against harm also increases as the severity of the possible harm increases. Accordingly, greater and more comprehensive measures are expected for systems with critical or sensitive data – or that are necessary to the operation of critical functions, such as medical services or electric power grids. Third, it is not necessarily a defense that many companies do not patch their systems promptly, or are even running unsupported software that cannot be patched. The U.S. Supreme Court articulated this principle a century ago:

> [W]hat usually is done may be evidence of what ought to be done, but what ought to be done is fixed by a standard of reasonable prudence, whether it usually is complied with or not.[32]

---

[32] *Texas & Pacific R.R. Co. v. Behymer*, 189 U.S. 468, 470 (1903).

In 1932, Judge Learned Hand made the leading statement of the rule, declaring that tugboat owners who sent their boats to sea without radios could be held liable for that practice even though no one else in the industry was using radios:

> [I]n most cases reasonable prudence is in fact common prudence; but strictly it is never its measure; a whole calling may have unduly lagged in the adoption of new and available devices. It never may set its own tests . . . Courts must in the end say what is required; there are precautions so imperative that even their universal disregard will not excuse their omission.[33]

III. The Risk of Liability

So far, there have been few computer security liability cases. This trend could continue. But we doubt it.

Cases. We are aware of only two significant cases involving failure to apply security patches – both in 2003 and both in a regulatory context. In April 2003, the Maine Public Utilities Commission ("PUC") denied the request of telecommunications company Verizon Maine for a waiver of performance standards on its network during January 2003 because performance had been degraded by "situations beyond [its] control" – namely the SQLSlammer worm.[34] The PUC concluded that because Verizon had failed to apply the security patch for SQLSlammer that Microsoft released six months earlier, it had "failed to act in a reasonable and timely manner to institute preventive actions."[35]

Even more telling, in June 2003, the U.S. Federal Trade Commission ("FTC") settled a suit against clothing retailer Guess. The suit alleged that Guess had unlawfully failed to protect

---

[33] *T.J. Hooper v. Northern Barge Corp.*, 60 F.2d 737, 740 (2d Cir.), *cert. denied*, 287 U.S. 662, 53 S. Ct. 220 (1932).

[34] *Inquiry Regarding the Entry of Verizon-Maine Into The InterLATA Telephone Market Pursuant To Section 271 of Telecommunications Act of 1996*, Maine Public Utilities Dkt. No. 2000-849 (Apr. 30, 2003) (Order).

[35] *Id.* at p. 5.

its customers' privacy because it did not "use reasonable or appropriate measures to prevent consumer information from being accessed at its Web site."[36] In particular, the FTC claimed that Guess had failed to repair website vulnerabilities (involving SQL injection attacks – related to the SQLSlammer attack) about which it had known since October 2000, resulting in a successful attack and theft of credit card numbers in February 2002.[37]

These cases are highly significant, in our view. One reason that courts and regulators have been reluctant to impose liability for computer security failures has been a sense that computer security is too fast-moving, too sophisticated, and too much a matter of judgment for lawmakers to set firm rules. But as these cases show, it is easy for a regulator to latch on to the question of installing patches and to say "Even I know that you have to do *that.*" It is an easy step from that view to the imposition of liability on companies that fail to install patches.

---

[36] "Guess Settles FTC Security Charges; Third FTC Case Targets False Claims about Information Security," FTC press release available at http://www.ftc.gov/opa/2003/06/guess.htm (June 18, 2003).

[37] There have been various computer security cases involving issues other than security patches. For example:

- Class action lawsuits were launched in early 2003 against Tri-West Healthcare and ISM Canada (a subsidiary of IBM), in the United States and Canada respectively, in unrelated cases involving theft of computer disk drives containing consumer information. *See* "Class-Action Lawsuit Filed on Behalf of Potential Identity Theft Victims," available at http://www.kold.com/Global/ story.asp?S=1105006 (Jan. 29, 2003); Paul Waldie & Jacquie McNish, "Missing computer disk spurs suit," *The Globe and Mail*, available at http://www.globeandmail.com/servlet/ArticleNews/printarticle/gam/20030204/RINVE (Feb. 4, 2003).

- The FTC reached a settlement with Eli Lilly in January 2002 regarding an e-mail error that resulted in 669 users of Prozac receiving each others' e-mail addresses, and a settlement in August 2002 with Microsoft regarding its security claims for the Passport authentication and wallet service. *See* "Eli Lilly Settles FTC Charges Concerning Security Breach," FTC press release available at http://www.ftc.gov/opa/2002/01/elililly.htm (Jan. 18, 2002); "Microsoft Settles FTC Charges Alleging False Security and Privacy Promises," FTC press release available at http://www.ftc.gov/opa/2002/08/microsoft.htm (Aug. 8, 2002).

- In August 2003, in order to comply with California SB 1386 (and to avoid a lawsuit), Arkansas-based database company Acxiom disclosed a security breach that compromised unencrypted information of California residents in its corporate customers' databases.

Indeed, the FTC's embrace of that idea could be particularly important. The FTC has a substantial influence over courts, legislatures, and other decision-makers, such as state attorneys general. And indeed, it is highly significant that both the Maine PUC and FTC in these cases found that the failure to apply security patches was not "reasonable" – since reasonableness is the key consideration for courts in establishing the duty of care in a negligence case.

Scope of the Duty to Patch. Assuming as we do that other policymakers adopt this shortcut to establishing a duty of care, what is its scope? Obviously, when a company is running a software product and the manufacturer releases a patch, the company needs a program for promptly installing the patch. Without such a program, liability is a real risk.

A somewhat harder question is how quickly patches should be implemented. In part that will depend on the size of the vulnerability and the urgency of the software producer's recommendation that the patch be installed. But it will also depend on experience. In particular, the speed with which past vulnerabilities have been turned into worms, viruses, or other malware. Here the bar may have been substantially raised by the Blaster worm's two-week turnaround from announcement of the security flaw (and release of the patch) to exploitation. As a result, there is a growing tension between the need to patch increasingly rapidly and the patch deployment difficulties discussed above. These deployment issues may themselves raise security and operational issues; and courts and policymakers will need to balance such competing considerations in deciding how quickly companies can reasonably be expected to apply security patches.

What if the company is running unsupported or outdated software? In that case, there will be no patch to install. But the lack of a patch will not necessarily excuse the company from liability. The most likely scenario is this. A piece of malware is released that exploits a security

flaw that can be found in both a current software product and in that product's no-longer-supported earlier versions. A company using the earlier version falls prey to the malware because no patch has been released. In a lawsuit, the plaintiff whose data was compromised or whose service was interrupted will argue that the company's patch plan should have identified programs that were no longer supported and should have upgraded to a supported version, either as a routine matter or, at least, when a patch was released and the company realized that the only way to install the patch was to upgrade its software. If the court concludes that installation of current security patches is part of the company's duty of care, it almost certainly will not accept as an excuse the fact that the software was so outdated that no patch was available.

As noted above, we believe that there is likely to be a significant increase in computer security cases over the medium-term – particularly if the major firms of plaintiffs' lawyers start to take an interest in the area. Indeed, the fact that many of the most significant cases have been initiated or decided in 2002 and 2003 suggests that an upward trend is already beginning.

Who Will Be Affected? In attempting to assess the areas of greatest liability risk with more specificity, we think that a couple of points are important. First, risks are greater from consumer lawsuits, including class actions, than from corporate lawsuits. Although computer security issues frequently arise in the business-to-business context, major computer security lawsuits between businesses are likely to be less common for a number of reasons, including that:

- most businesses are reluctant to allow a commercial relationship be disrupted by a lawsuit;
- many contracts disclaim liability for security breaches, and such disclaimers are likely to be enforced between businesses (although some contracts are beginning to address security obligations with increasing specificity); and

- the largest risk from security breaches is usually compromise of data regarding individuals (credit card numbers, medical information, etc.), and individuals (likely acting through class counsel) are more likely to seek damages for such breaches than are the businesses that hold or process the data.

All that said, the risk of business-to-business conflict remains real. Once the ice is broken, disputes among businesses may become serious. For example, in a consumer security-breach lawsuit, the defendants are likely to include the company whose name is on the door plus any outsourced service providers that actually handled the company's communications or IT services. These defendants will likely end up suing each other as well in an effort to pin the blame elsewhere. Even when litigation is not triggered by consumers, a serious security breach by a contractor will at the least lead to reconsideration of the contract and quite probably to financial compensation determined through litigation, arbitration, or just hard-nosed negotiation. Finally, securities class actions, which lie at the border between consumer and business lawsuits and have become a major corporate liability issue in the last 15 years, are also a risk if the fallout from a security incident includes a significant drop in the price of a company's stock.

Second, the industry sectors most at risk may be counter-intuitive. For example, financial institutions are subject to extensive security regulation and have hard cash at risk from security breaches. But it is not clear that their risks from computer security litigation are particularly high, in part because consumers' financial rights are very clearly defined, and in part because financial institutions (or at least banks and credit card issuers) have generally absorbed the cost of consumers' losses from security failures. Only if a financial institution refuses to make good such losses is it at severe risk of a lawsuit.

Rather, litigation risks may turn out to be higher for entities like large retailers that hold large amounts of consumer data. Compromise of such data by an unknown attacker could

produce significant and uncertain damage, due to risks like identity theft. It is just such an uncertain liability situation that makes litigation most likely.

Insurance. A particularly significant risk from failure to implement security patches relates to insurance. A few years ago, it was difficult to buy affordable insurance for computer security risks. But as the insurance market has begun to understand such risks better,[38] insurance is increasingly available. However, standard insurance policies may not apply where the insured fails to implement available security patches. For example, the AIG netAdvantage Security[SM] policy excludes coverage for losses "due to installing or failing to install a software patch."[39] The likelihood or possibility that particular conduct could lead to uninsured liability should have a significant effect on behavior with respect to such potential liability.

IV. Conclusions and Best Practices

There is a growing risk of liability for companies that run software without a process for promptly installing appropriate security patches, and very likely for failing to update software that is no longer supported and has known security vulnerabilities. Indeed, the risks of such liability appear to be increasing rather quickly, for reasons that include increased incidence of security breaches resulting from failure to install patches, increased legislative and regulatory attention to security issues in the post-September 11 environment, and a general increase in information technology regulation as the market moves from Internet boom to bust to business as usual.

---

[38] At least the insurance market appears to believe that it understands such risks. We believe that the increasing likelihood of computer security litigation discussed in this article may have some rude surprises in store for the insurance market.

[39] The fact that the exclusion extends to losses resulting from both installation of and failure to install software patches places insureds in a difficult position, requiring them to install patches, but do so in a fashion that does not disrupt existing operations. Presumably, this requires timely and careful testing of patches in the insured's computing environment.

As in other areas of law, adoption of company policies based upon industry best practices can significantly mitigate potential liability. We believe that a best practices security patch policy should involve at least the following elements:

- implementation of available patches to address vulnerabilities that are (1) publicly identified by CERT (and/or other sources like DHS) and/or (2) notified by a manufacturer of software;

- ensuring that such implementation takes place on a timely basis, subject to deployment concerns like those discussed in section I above – *e.g.*, ensuring compatibility of patches with the existing computing environment (and pursuit of alternatives where compatibility issues are identified);

- rapid replacement of software, particularly software that has significant known security vulnerabilities (identified by CERT, the manufacturer or other sources) for which patches are not available; and

- specific implementation of statutory and/or regulatory requirements applicable in a given sector (especially health care or financial services).

The details of such a policy would of course depend upon the circumstances of the particular company or organization, including because security commitments that are made explicitly by contract may require specific procedures.

Although no reasonably feasible security policy can eliminate the possibility of computer security breaches, companies that adopt and follows security policies based upon best practices should be able to moderate and insure against such risks, particularly those of a catastrophic nature. In particular, it is likely be fairly difficult for government regulators, potential class action plaintiffs, or others to pursue claims based upon implied contract or negligence against companies that follow best practices in the security area.