VOLUME TWO · ISSUE THREE
Secure Business Quarterly:
Defining the Value of Strategic Security

SBQ

THIRD QUARTER 2002
Exclusively on the Web at:
www.sbq.com

SECURE BUSINESS QUARTERLY

ILLUSTRATION: RON CHAN

Vulnerability Disclosure

Whom Does it Serve?

Legal Framework Needed for Vulnerability Disclosure Liability

by Jane Winn

Secure Business Quarterly℠ is an @stake® publication.

Legal Framework Needed for Vulnerability Disclosure Liability

by Jane Winn

ILLUSTRATION: JAMES STEINBERG

If the disciplines of computer security theory and practice are now enjoying a post-September 11 Renaissance, the discipline of computer security law remains mired in the Dark Ages.

Once again, technological and economic developments are giving rise to conflict and spawning disputes at a much faster tempo than lawyers can process them. Given the rudimentary level of development of computer security law in general, it should come as no surprise that the law has not yet developed a coherent, rational response to conflicts created by the practice of vulnerability disclosure.

The Digital Millennium Copyright Act of 1998 (DMCA) is one of the few laws created by legislation or judicial precedent that might clearly apply to conflicts created by third party vulnerability disclosures. However, the DMCA was created to protect the rights of publishers, not to promote the development of security information systems outside the context of rights management systems. As a result, the regulatory regime created by DMCA is too simple and narrow in focus to promote responsible vulnerability disclosures or vulnerability remediation.

The DMCA grants sweeping new privileges for copyright owners with regard to rights management systems and anti-circumvention technologies, imposing new liabilities on anyone who frustrates the exercise of those privileges. However, in order to avoid choking off legitimate research into encryption technologies and information system security, the DMCA recognizes limited exceptions to these new liability rules for research. 17 U.S.C. 1201(g) and (j). The scope of these exceptions is a matter of some controversy (as demonstrated in the recent cases involving Edward Felton of Princeton University and Dmitry Sklyarov of Elcomsoft). To be covered by the encryption research or security testing

continued…

Legal Framework Needed for Vulnerability Disclosure Liability
(continued)

Technical standard setting efforts might be a more informed and responsible source of vulnerability disclosure liability rules than legislatures or courts

exemptions, the access must have been authorized. A restrictive provision in a shrink-wrap or click-wrap license agreement could negate the effect of the statutory exemption. Assuming authorized access is not an issue, the disclosure must be made in a manner that does not facilitate copyright infringements.

A rational regulatory regime for vulnerability disclosure and remediation could lower the overall cost of ensuring adequate levels of security by encouraging optimal levels of investment in information security. Such a regime would have to define standards of conduct for product developers, end users and third parties such as reporters or researchers that have legitimate interest in disclosing vulnerabilities and should be amenable to incentives to do so responsibly. No such regime exists today, and it is not clear whether even well-informed, well-intentioned legislators could write a statute today that would achieve all these ends. In the absence of existing legislation or case law, the most obvious source of new law in this area is likely to grow out of tort doctrines such as negligence.

Lawyers are increasingly interested in the question of when the owner of an information system might be liable for harm caused to third parties due to a failure to maintain adequate security. (This interest may stem from the turn of the century. Many lawyers became computer literate to better handle a myriad of Y2K cases that never materialized and have been casting about for some time trying to find alternative uses for that knowledge.) Even if a legal standard were to be developed quickly to resolve this issue, it would shed little or no light on the question of when a third party disclosing a vulnerability should be liable either to the developer of the product in question or to end users of the product. Such liability might be based on negligence if the manner in which the disclosure is made fails to (1) minimize the ability of malevolent third parties to capitalize on the disclosure and (2) maximize the ability of parties with legitimate interests in the product to fix the problem.

Negligence law is traditionally developed one case at a time, and is a process that may take years or decades. It is unlikely that the courts will be able to develop, in a timely fashion, a sophisticated framework for analyzing the rights and responsibilities of developers, end users and third parties such as reporters with regard to vulnerability disclosure or remediation. A quick perusal of recent federal legislation aimed at cyberspace, including the DMCA or the Electronic Signatures in Global and National Commerce Act (E-SIGN), or state legislation such as the Uniform Computer Information Transaction Act (UCITA) supports the lack of confidence many computer security professionals have that a such a rational regime is likely to appear on the horizon any time soon. The relative ineptitude and sloth of legal institutions in this type of arena, where a high level of technological sophistication is an essential prerequisite to informed discussion and action, indicates that future law reform efforts are likely to be similarly flawed.

Technical standard setting efforts might be a more informed and responsible source of vulnerability disclosure liability rules than legislatures or courts. Technical standard setting efforts have their own shortcomings, and may be vulnerable to the same problems of political capture or bureaucratic ineptitude that plague legislatures and courts. In the context of vulnerability disclosures, however, they might produce more rational outcomes than legal institutions because of the greater technological sophistication of their participants as well as the more limited scope of their focus. SBQ

Jane K. Winn is Shidler Center for Law, Commerce & Technology Professor of Law at the University of Washington in Seattle. She is the coauthor of the treatise Law of Electronic Commerce, 4th edition (2001), and the textbook Electronic Commerce (2002