

Lawsuit Challenges Wall Protecting Software Vendors From Liability

Richard Hunter

A California woman has sued Microsoft; she alleges that flaws in its software caused her to be victimized by identity theft. Gartner believes that the liability of vendors for flawed software will be legally established by 2007.

NEWS ANALYSIS

Event

On 30 September 2003, a woman filed suit in a California court against Microsoft (see "Lawsuit Against Microsoft May Help Computer Security"). She alleges that a criminal exploited vulnerabilities in the vendor's software to steal her identity. The plaintiff and her lawyers plan to turn the case into a class-action lawsuit by showing that a large group of people have suffered through Microsoft's alleged negligence.

Analysis

As technology spreads throughout society, the issue of security follows. It comes to the top of people's minds when 3.4 percent of U.S. adults fall victim to identity theft annually (see "Study Shows Financial Firms Need to Act Against Identity Fraud"). In a survey conducted by Gartner in June 2003, a vast majority of respondents favored holding software vendors (and other companies writing software for customer use) legally liable for flaws in their products. (The respondents also rejected government regulation of software quality.) Legislation (such as California's Database Security Breach Notification Act) increasingly holds companies liable for security breaches, and Gartner expects that enterprises will seek to shift their liability onto software vendors.

Microsoft's products are among the first targets for legal action because they are widely used and widely attacked. This lawsuit alleges that Microsoft's monopoly status eliminated the plaintiff's opportunity to choose alternative software products and that therefore the standard license terms disclaiming Microsoft's responsibility for damages resulting from flaws in its software are unenforceable. The lawsuit stops short of claiming that the license terms themselves, which are standard for the software industry, are intrinsically unenforceable. This probably offers a temporary refuge for software companies that don't happen to be monopolies. Microsoft has spent well over \$100 million since 2002 to improve the quality and security of its products, with some success, but attacks occur with increasing frequency (see "Worm Outbreak Shows Need to Keep Paying for Security"). Clearly, the plaintiff in this case does not feel that progress has been rapid enough.

This type of lawsuit needs time to work through the legal system, and the outcome is unclear. Legal precedents have yet to be set. Software vendors have moved to reduce their legal liability by writing strict end-user license agreements. Nevertheless, this lawsuit puts the industry on schedule to confirm Gartner's forecast:

- By 2007, widely accepted legal norms for assessing civil damages resulting from negligent IT security will have been established in the United States by statute or by case precedent (0.8 probability).
- By 2008, at least one such lawsuit will result in a judgment or settlement for more than \$10 million in favor of the plaintiffs (0.6 probability).

This trend gives enterprises another reason to implement sound patch management and software development processes — eventually, failure to keep up with recommended fixes to known vulnerabilities may result in legal liabilities.

Analytical Source: Richard Hunter, Gartner Research

Recommended Reading and Related Research

- "Force Vendors to Make Software More Secure" — Flawed software poses perhaps the single greatest security problem for industries, governments and consumers; therefore, enterprises should demand that vendors take more responsibility for the security of their software. **By Arabella Hallwell and Rich Mogull**
- "A 'Bill of Rights' for Software Buyers" — The U.S. Congress and other legislatures, along with regulators and the courts, should stipulate certain software buyers' rights and spurn industry attempts to support legislation that diminishes these rights. **By Tom Austin**

(You may need to sign in or be a Gartner client to access all of this content.)

REGIONAL HEADQUARTERS

Corporate Headquarters

56 Top Gallant Road
Stamford, CT 06902-7700
U.S.A.
+1 203 964 0096

European Headquarters

Tamesis
The Glanty
Egham
Surrey, TW20 9AW
UNITED KINGDOM
+44 1784 431611

Asia/Pacific Headquarters

Gartner Australasia Pty. Ltd.
Level 9, 141 Walker Street
North Sydney
New South Wales 2060
AUSTRALIA
+61 2 9459 4600

Japan Headquarters

Gartner Japan Ltd.
Aobadai Hills, 6F
7-7, Aobadai, 4-chome
Meguro-ku, Tokyo 153-0042
JAPAN
+81 3 3481 3670

Latin America Headquarters

Gartner do Brazil
Av. das Nações Unidas, 12551
9º andar—World Trade Center
04578-903—São Paulo SP
BRAZIL
+55 11 3443 1509