A Warranty of Cyberworthiness

In an earlier Application Security installment (“The Case for Software Warranties,” May/June 2003, pp. 80–82), Martin R. Stytz reasoned that before customers will purchase and use new, expansive, and ubiquitous computing products, they want reliable assurances that the processing software

will protect sensitive and confidential data entrusted to it. His premise was that “users must know with certainty that their data is secure, that they control each application at their service, and that their privacy is protected.” In short, he asserts that such users will demand security warranties.

Unfortunately, if security warranties were to be added to a software license, they would appear too absolute and unlimited. We are not about to achieve absolute computer security for devices linked to cyberspace. And even if we could, the requisite sacrifices in privacy would be unacceptable. Stytz acknowledged that the security he envisions is “far from being realized.”

In his department, Stytz described a hypothetical user of computing devices, located in an imagined time of the not-too-distant future. Such a user is more critical of security than most current users are, and more likely to condition a purchase on receipt of reliable security assurances. In this response to Stytz’s viewpoint, I start with a different premise and pursue a more limited and feasible objective. I also start with a user in the present. (A more detailed version of this article is available at <http://lawplace.metadot.com>.)

A cyberworthy warranty

Today, most users are rapidly expanding their use of computing devices and software despite compelling evidence that doing so with networked cyberspace computers provides ever-increasing risks of security breakdowns that can result in unauthorized access or disclosure of confidential information. Users fear that they have no choice but to link their computing devices via cyberspace, despite the perils it poses. All such users want the absolute security Stytz described, but as long as that remains unattainable, they are not in a position to bargain and negotiate to receive warranties of absolute security.

Currently, software makers resist offering cybersecurity warranties, and will continue to do so if the only one they consider is the unattainable absolute security they can’t, in good faith, cover with an unlimited warranty. But what if the warranty were something less ambitious, more immediately attainable, and more beneficial (for both customers and makers)?

Let’s explore the possibilities of a written warranty that vouches for an application’s capabilities to protect confidential information from unauthorized access from, or disclosure to, cyberspace—a warranty

of *cyberworthiness*. Software makers have much to gain if they consider offering a limited warranty that addresses their customers’ most manageable, serious concerns. Software makers also must respond to a recent critical change: a substantial time reduction between their issuing a security patch and the hackers’ launching exploits against the disclosed vulnerability. Software makers no longer can justify a simultaneous patch release to all users; it leaves confidential information too exposed to hackers’ rapid reactions.

Mindful of those considerations, a provisional draft of a limited cyberworthiness warranty might state:

- Prior to the software’s release, the maker subjected it to rigorous tests to verify its degree of security against intrusion by unauthorized persons, electronic agents, or code (that is, it verified its cyberworthiness).
- By the time of release, the maker removed all known critical security vulnerabilities found in the software. (I define “critical” as any vulnerability that, if exploited, would enable unauthorized access to confidential information or unauthorized control of a user’s computing device.)
- After release, the maker shall continue to diligently probe the software for security vulnerabilities.
- When the maker learns of a critical vulnerability, it will immediately email all high-priority customers, describe the problem in detail, and provide suggestions for a temporary solution—disabling features, and so on—to diminish or limit the vulnerability until the maker can

ROLAND L.
TROPE
*Trope and
Schramm LLP*

provide a patch. (“High-priority customers” are those likely to have valuable confidential information at risk in systems linked to cyber-

computing device’s warranty. It should be a period long enough to earn a user’s trust. A 90-day or six-month warranty is far too small to

As a ship fit for sea duty risks is deemed seaworthy, software fit for the cybersecurity risks should be considered cyberworthy.

space. To become such a customer, the party would enter into a written agreement with the software maker that any vulnerabilities disclosed and patches released to it would be kept confidential to prevent hackers from gaining early knowledge of such vulnerabilities. These customers would pay an increased purchase price in exchange for the incremental increase in protection.) The vulnerability notice also would include information that would alert users to take additional precautions to safeguard their confidential information until they had received a security patch.

- Immediately after creating a vulnerability security patch, the maker would email it first to the high-priority customers and, after an interval, to all registered software users.
- When distributing a security patch, the software maker shall not attach to it any disclaimer as to the accuracy of information provided with the patch or its fitness for correcting the specified security vulnerability. This is not a warranty for fitness for any particular purpose—except security against intrusion from cyberspace—and it would be given in place of any warranties that might be implied by law, all of which would be disclaimed.
- The software’s warranty will be valid for a period of three years from the release date. (A security patch or newly marketed software should be warranted for a period comparable to that covered by the

earn much trust.).

- The warranty would be valid for purchasers who buy directly from the maker and for those who buy from third-party sellers, but still in the direct chain of distribution from the maker.
- The warranty would prescribe precautions to which purchasers must adhere, such as “do not open unknown attached files in emails from unknown senders.” Purchasers who violate the precautions (and suffer or cause harm) void the warranty, and will not be entitled to damages from the maker.
- If the maker breaches the warranty, the purchaser (buyer or licensee) is entitled to an expeditious remedy of a liquidated damage in an amount and through a procedure specified in the warranty. (High-priority customers would negotiate the amount of liquidated damages, while individual purchasers would be entitled to a fixed sum of, say, \$100, that they could receive by applying to an ombudsman appointed by the software makers.)

I crafted the proposed warranty, in part, by an analogy to warranties of ventures on the high seas. Those endeavors involve severe risks to property, limb, and life. A ship’s officers are assiduous in checking their vessel, before casting off, to verify its seaworthiness.

Under US common law, a ship is considered *unseaworthy* when it is “insufficiently or defectively equipped.”¹

Courts have come to regard the seaworthiness of a ship as analogous to a warranty,² a warranty implied not just for the vessel’s capability to traverse the high seas, but for conditions on board that might imperil crew members.

As a ship fit for sea duty risks is deemed *seaworthy*, software fit for the cybersecurity risks should be considered *cyberworthy*. As ship owners impliedly warrant that a vessel is seaworthy and are liable if its failure to be causes loss or damage to ship or crew, so I propose that software makers who insist on retaining ownership of their wares (by licensing copies to users instead of selling all rights to the software) should recognize that they invite users to deploy their software in links to cyberspace and should expressly warrant that such software is fit for such use—a warranty of cyberworthiness.

Devils in the details

The proposed warranty should be phased in, not with the software’s initial release, but with the first security-patch release. In doing so, makers would offer only the portion of the proposed warranty that applies to each patch. The warranty thereby would address first software makers’ inconsistent positions: warning of critical vulnerabilities, recommending corrective-patch implementation, inviting users to trust the patch, but then disavowing any responsibility for the information’s accuracy or the patch’s effectiveness.

What would or would not constitute a warranty breach? Software makers would not be in breach merely because a hacker found and exploited a vulnerability before they discovered and sealed it; otherwise the warranty would put an additional weapon in the hands of hackers intent on injuring the software maker.

However, software makers realize (and courts will hold them accountable that they should have foreseen) that the longer they take to discover a critical vulnerability and patch and

seal it, the more opportunities hackers have to exploit it and jeopardize customers' confidential information. Thus, the longer makers take to discover and correct a critical vulnerability, the more they risk being held liable for negligent discharge of their warranty obligations.

Software makers should anticipate that courts eventually will be asked to interpret the warranty if makers:

- don't dedicate ample resources (talent and funds) to finding critical vulnerabilities (a breach);
- don't immediately provide their high-priority customers with vulnerabilities notices and patches, when developed (a breach);
- discover a critical vulnerability that could imperil its high-priority customers' confidential information and pursue anything less than an urgent approach to patch development (a breach); or
- don't dedicate resources to such tasks proportional to the risks and the stakes (a likely breach).

There would be no breach, however, if the maker did not have reason to know that a critical vulnerability existed in the initially released software. Makers thus would not be liable for being sabotaged by a determined hacker, or obliged to win every security race against hackers. The warranty's aim is to motivate them to make cybersecurity a high enough priority that it will permeate the software code, minimizing the number and criticality of its vulnerabilities to intrusions and damage.

Liability on the horizon

If security problems continue to increase in frequency and severity, courts could become receptive to arguments that software makers should be liable for damages caused by software they knew, or had good reason to know, was not cyberworthy. Courts can reach that conclusion with no warranty involved, and

might award far more damages in that event. If software makers take too long to find critical vulnerabilities or to develop and release corrective patches, the courts might scrutinize their reasons and hold against them their failure to accept certain responsibilities, including:

- software security vulnerabilities resulting from the maker's code design;
- security vulnerabilities that are in the makers' own property because they retain intellectual property ownership in their software (they do not sell their wares, but only license them);
- by licensing software with the express purpose of making it available for use in processes linked to cyberspace, makers continue to create and benefit from a new class of "invitees" (users who have been invited to exploit in cyberspace the benefits offered by the software); and
- having created this class of invitees, makers incur a responsibility—susceptible to definition and limits—to ensure that their software does not unreasonably expose users' confidential information to cyberspace's perils.

We might be reaching the point at which the increase in computer system breaches and escalating damage costs cause a tectonic shift in purchaser priorities. The dam-

the US.³ Corporate management and public companies' boards of directors are not likely to let such risks continue to escalate without seeking to safeguard their companies' most valuable information assets.

That customers can be wooed (or wowed) enough to be distracted from security concerns, or to rank security as a lower priority than an immediate gain in performance capabilities, should not cause us to overlook three salient, countervailing tendencies. First, as security breaches and damage to confidential information intensify, commercial customers will react, ranking security a higher priority. Eventually customers will stop purchasing a product if its security can't be reliably assured. Second, some makers will perceive the shift in priorities, see it as an opportunity, and offer a limited warranty—namely, that their software does not contain any unreasonable vulnerability to the perils of cyberspace. They will warrant, with savvy simplicity, that it is cyberworthy. Third, customers, when offered the choice between software warranted to be cyberworthy and software without that warranty, will purchase the cyberworthy ware.

Mutual benefits and responsibilities

Although there will be details to iron out, anticipating them shouldn't prevent software makers from seeing the

Corporate management and public companies' boards of directors are not likely to let such risks continue to escalate without seeking to safeguard their companies' most valuable information assets.

ages from viruses and other computer crimes reportedly now averages US\$803,000 per company in

proposed warranty's advantages. Offering a cyberworthiness warranty is simply good business: good for win-

ning customers and market share, improving brand reputation and value, and for averting liability.

Of course, the cybersecurity problem doesn't exist solely because software makers produce flawed wares. Many exploits depend on inadvertent user complicity. Recent viruses and worms would have had little, if any, effect had individuals adhered to good security practices when faced with emailed messages. In the near future, firms that do not promptly implement a security patch for a widely reported vulnerability will risk being held liable for the consequences. A security patch's immediate implementation, however, might not be every firm's most prudent action. The patch might cause a system to operate erratically or crash. Software makers, intent on improving their wares' cybersecurity, should not be held responsible for knowing whether a security patch will conflict with substantially modified systems or those with customized, unique features. (The vendor never can know for sure what users put on their desktops—nor would we want vendors to have access to such information in exchange for the severe loss of privacy.)

As users should become more responsible when handling email with potentially pernicious attachments, so software makers should become more responsible for protecting users' confidential

information. In the tripartite relationship among software makers, users, and hackers, makers and users should each be seeking to shore up their security practices, because each is likely to be held liable for shortcomings that let a hacker's malware detect and exploit a critical vulnerability. If software makers warrant their wares' cyberworthiness, then customers, too, might well respond by improving their precautions (to preserve their rights under the cyberworthiness warranty and to secure their systems). By issuing a cyberworthiness warranty, software makers could initiate an iterative process that moves an ever-increasing number of computing devices further along the spectrum toward reliable security for confidential information.

Until then, security breaches will intensify. Widely reported exploits will be surpassed by intrusions and theft of, or damage to, confidential information that might go undiscovered for months. It would not be wise for software makers to wait until a calamitous loss brings courts to rule that the era of security flaws without liability has ended (just as courts decades ago eventually ruled that a similar era for defective autos with no liability for their makers had ended).

The US Federal Trade Commission already advances the principle that—even without a security breach—there can be violations of law where the software maker provided insufficient security to back up its promises. The FTC maintains that, in that event, a maker has a “legal obligation to take reasonable steps to guard against reasonably anticipated vulnerabilities.”⁴ Therefore, it filed a complaint against Microsoft for failing to provide sufficient safeguards to protect the privacy and confidentiality of personal information (including credit card numbers) obtained through Passport and Passport Wallet.

Software makers can't avoid in-

definitely the choice between court-imposed liability after serious damage and the far more limited (and self-circumscribed) liability that might be incurred if a maker breaches the proposed warranty of cyberworthiness. It would be prudent to choose the warranty while the chance to choose still exists. A mere commitment to enhanced security in the next version of a maker's wares will not suffice. □

Acknowledgments

Views expressed herein are solely those of the author, and not of the US Military Academy, Department of Defense, or government. For their criticisms and suggestions on this article, the author thanks Elliot Brown, Leonard Goldberg, John Gregory, Lynne R. Malina, Charles Montagne, Louise Nemschoff, E. Michael Power, Chuck Resor, and Konrad Trope.

References

1. *Waldron v. Moore-McCormack Lines, Inc.*, 386 U.S. 724, 726 (1967).
2. *Brister v. A.W.I., Inc.*, 946 F.2d 350, 355 (5th Cir. 1991).
3. E. Rapp, “Demand for Workers Surges In Policing Cybertechnology,” *The New York Times*, 15 Feb. 2004, sec. 10.
4. “Cybersecurity and Consumer Data: What's at Risk for the Consumer,” Prepared Statement of the Federal Trade Commission, 2003; www.ftc.gov/os/2003/11/031119swindletest.htm.

Roland L. Trope is a partner of Trope and Schramm LLP, and adjunct professor in the Department of Law at the United States Military Academy, West Point. His research interests include cyberlaw, export controls, cybersecurity, and privacy protections in cross-border transactions, intellectual property, and linguistics. He has a BA in political science from the University of Southern California, a BA and MA in English language and literature from Oxford University, and a JD from the Yale Law School. He is a member of the IEEE, the American Bar Association's Cyberlaw Committee, and the Association of the Bar of the City of New York's Information Technology Committee. Contact him at roland.trope@verizon.net.