**Needed: A Security Blanket for the Net**
*by Alex Salkever, Technology editor for BusinessWeek Online*

Worms, viruses, bugs, spam, and hackers have spurred many experts to start pushing concrete reforms, some quite radical

David Farber, a computer science professor at Carnegie Mellon University in Pittsburgh and a regular speaker at high-tech confabs, has long been a cheerleader for the Internet. In that capacity, he manages a rollicking free mailing list called Interesting People that links its thousands of readers to Web pages he thinks the digerati will find appealing. Farber's audience is a microcosm of the Internet -- people from all walks of life wandering in and out of conversations and sharing information with those who until moments before were strangers.

This summer, though, as computer bugs and worms infected anything linked to the Net, Interesting People developed a funereal air. Reader after reader complained that it was becoming harder to use the Net constructively. As spam filled in-boxes and viruses crashed networks, the Net seemed to cross a threshold from controlled anarchy to utter chaos, readers said.

Farber himself joined the chorus. "This summer, if I had been on the end of a 56 kilobit [dial-up] line, I would have used my PC as a giant paper weight," he wrote at one point. "When you get to that point, you start to wonder if this is all worthwhile." That's a shocking statement from someone who first used the Net in the 1970s, when it was part of a military research project.

WAKEUP CALL. The tide of bad behavior on the Web has been rising for some time, of course, and reactions such as Farber's aren't unprecedented. Still, this summer's security breakdowns were a wakeup call for even the medium's most devoted fans, who are reaching a broad consensus that something must be done to fix the Net. "We are now at a pain point where we would contemplate solutions that are more involved than we would have imagined 12 months ago," says Leslie Daigle, chairperson of the Internet Architecture Board (IAB), an international nonprofit group that helps set policy for the self-governed, unregulated Internet.

The steps her group is advocating range from legislation that would let customers sue software companies over security loopholes in their products (by law, the industry is now largely exempt from such claims), to building new tracking systems that would make it impossible for even hackers to use the Internet without leaving a clear trail, to forcing everyone on the Net to put security protection on their PCs.

Every remedy has a downside -- usually, it boosts costs or reduces privacy -- and each will be hard to implement without somehow damaging the Net as it has been so far. And yet, it seems clear that the Internet has grown so far beyond its geek roots that it has "truly come to resemble society with both the good and the bad," Farber says. And a realization is growing that it may need to be managed with that foremost in mind.

"SOMEWHAT FLAKY." Fortunately, despite the recent debacles, the Net's underpinnings remain solid. Generally, network performance has stayed strong, and traffic has continued to grow. In October, 2002, the so-called DNS root servers -- the 13 systems containing the databases that are the highest-level cops for directing traffic around the Internet -- survived a massive denial-of-service (DOS) attack without failing, an event many observers took as proof that the system remains robust.

This summer's SoBig intruder, though one of the most virulent worms yet, failed to shut down the Net, even though it triggered a 20-fold increase in requests for mail-server lookups at DNS root operator VeriSign (VRSN ). The Web even has a sort-of safety net: a glut of fiber-optic capacity around the world that could be used if the current pipes start to clog. And yet, as the Net has become more widely used, "things...have gotten somewhat flaky," worries Farber. He argues that

ensuring the security of computers and systems should be the No. 1 priority for protecting the Net and those who use it.

The most technically radical proposal that's being advanced would alter the way data is exchanged on the Net, with the aim of making the passage of bits and bytes much less anonymous than it is now. It's this namelessness that creates a haven for hackers who forge or spoof the originating IP address (an Internet identification tag for computers) on their data to mask their identity.

VALIDATING TRAFFIC. Spammers, too, love the faceless nature of the Web since it gives them cover as they send millions of messages with bogus address headings. The solution, say some, is to build in mechanisms for identifying and authenticating anyone who uses the Net. The goal would be to legitimize an environment where, at the moment to some extent, engaging in "commerce is the moral equivalent of buying a watch from someone in a trench coat on a street corner," says the IAB's Daigle. "We need better accountability."

That could take several forms. The newest iteration of the Internet protocol standard, called Ipv6, provides a way to assign tracking tags to data that move over the Net. Paul Mockapetris, who helped design the current DNS system, has suggested combining this capability with a more secure form of DNS, called DNSec, that uses digital certificates stored on machines connected to the Internet to validate that the data passing across the wires originated from those servers. If this worked as advertised, those who dispense worms and viruses would be unmasked -- or at least thwarted.

Several other technical ways exist to achieve this aim. Unfortunately, all would require some heavy lifting -- namely, widespread adoption of new DNS and routing software that's harder to use than the existing variety. And managing all the digital certificates or encryption keys -- nearly every PC would need to have one for these proposals to work -- would likely prove onerous, boosting the costs of both software and training.

LEGALLY LIABLE? "Ipv6 has been out for some time, and almost no one uses it in commercial deployments" for such reasons, says Jerry Brady, chief technology officer of information security company Guardent in Waltham, Mass. Moreover, eliminating anonymity has a downside: While it might hamstring hackers, it would also do the same to human-rights activists who use the Net's nameless nature to communicate important information from dangerous places -- without putting themselves in jeopardy.

Other advocates of stronger cybersecurity see the issue in legal terms. They argue that broadening the rights of companies and individuals who've been harmed by software glitches to sue for damages would enforce better discipline and security in everything from Web deployments to software design. That would make the likes Microsoft (MSFT ), IBM (IBM ), Sun Microsystems (SUNW ), Oracle (ORCL ), and Computer Associates (CA ) more liable for fending off worm outbreaks or fixing software flaws -- liability they escape at the moment, thanks to the user agreements they require customers to sign that free the industry of such responsibility.

"People who make money on selling the software are the ones to pursue," argues Guardant's Brady. "The fact that a 14-year-old can write a worm that can take down a good portion of the Internet shows that the software guys aren't doing a good job." Such a legal shift would also likely open up banks and credit agencies to damage suits over security breaches that yield personal information to digital intruders.

NEW RULES. Creating tougher network-security guidelines and then putting the full faith and power of the government behind them would help, too, say some security experts. Examples of that are the Financial Services Modernization Act of 1999, which mandates better privacy for customers of the financial-services industry, and the Health Insurance Portability & Accountability

Act of 1996, which requires the same of hospitals and health insurers. Both laws have spurred considerable thinking about -- and investment in -- ways to improve security.

"The only way we've seen this happen [in the past] is through regulation," says Brady. "Regulation has changed the way those enterprises look at risk management. They now understand that if they don't adapt, the U.S. government will punish them."

Still, Brady concedes that regulation has its limitations: It may work in the U.S., but the Web is an international medium. And comparing buggy software to, say, defective tires, isn't entirely fair. Microsoft operating systems contain tens of millions of lines of code and are hopelessly complex, in part because they have to be compatible with previous versions of the software in order to keep the 95% of the computing world that uses them happy.

PLENTY OF BLAME. Microsoft claims -- and Farber believes -- that the bugs of yore have been conquered. "When I was running old mainframes," Farber recalls, "when we got a new piece of software, we would put it in a drawer and only test it after we stopped receiving a telegram a day telling us about a new bug." In fact, it's unlikely that even the most draconian regulation could eliminate bugs unless accompanied by significantly upgraded discipline on the part of thousands of programmers who routinely make unauthorized code changes on networked computers as a shortcut, or simply to achieve an objective they've been given.

In some instances, Internet service providers and network administrators deserve as much blame for security breaches as anyone else. Many of them have regularly failed not only to ensure that their machines have the latest patches from software companies -- as was the case with the MS Blaster worm outbreak in July -- but also to take basic steps that would prevent dangerous data traffic from crossing their networks.

"No. 1 on my list would be to put access-control lists on all your routers and switches to prevent any spoofing [by hackers] of source IP addresses," says Paul Froutan, vice-president for engineering at San Antonio Web-hosting company Rackspace. Such lists, he explains, would filter out traffic that makes bogus use of IP addresses he manages. "It would take some effort," Froutan says, "but it wouldn't cost millions of dollars."

"KNEE-JERK REACTIONS." Problem is, adding too many such restrictions can be a double-edged sword, says the IAB's Daigle. She points to the common ISP practice of blocking mail sent by customers that isn't directed through the ISP's own mail servers. Spammers use this trick to blast millions of messages without being caught. But Daigle herself likes to send mail that way because she can select more secure servers and encryption protocols than a typical ISP offers.

"That's an example of appropriate behavior blocked by a reactive technique," she says. "If we apply some of these knee-jerk reactions, we end up with a very restricted network that won't be functional for anyone's needs."

Whatever the strategy, improving Net security will almost certainly have to involve consumers as well as business. The majority of infected machines that barraged Web servers with SoBig e-mail were home computers connected to the Net via broadband. "Right now, the people who own the Internet are a few million AOL users who don't necessarily care about security," says Guardent's Brady. To date, most efforts to get consumers to be more security-conscious have amounted mainly to exhortations for them to lock down their desktops and laptops with firewall and antivirus software -- along with calls for better education of consumers.

SAFETY AS A SERVICE. Some security hawks say broadband providers should take more responsibility for the risks posed by consumers -- and not even accept customers unless they have security software installed on their PCs, software that perhaps should be provided by the

ISP. Such talk doesn't thrill big ISPs, which claim to do their best to keep customers informed on security matters without alienating them.

ISPs have an upside, though: They can make money on security. AOL (AOL ) offers an antivirus service that screens e-mail and can scan a customer's hard drive for viruses and worms -- for $3 per month. Cable-broadband providers Cox Communications (COX ) and Comcast (CMCSA ) offer similar services, with the first year free but with the implication that customers will have to pay thereafter. AOL has rolled the cost of a consumer firewall into its $55 broadband access package, effectively levying a security tax on subscribers.

Of course, repeated recurrences of severe Internet security breaches could make everyone move more aggressively. That day may well be coming. Scott Schell, a senior vice-president for marketing at security and authentication software company RSA Security (RSAS ), believes the most pernicious threat isn't in attacks that inconvenience all Net visitors, such as spam, worms, or DOS assualts. Nor, he says, is the biggest threat piecemeal hacking aimed at harvesting credit-card numbers from eBay (EBAY ) users.

"POT OF GOLD." Rather, Schell worries most about the security of big databases that store huge amounts of personal information for millions of Americans. Often, government and commercial databases contain a treasure trove of info, more than enough to steal an identity. "If someone can compromise [credit-report company] Equifax (EFX ), they reach the pot of gold in the hackers paradise," says Schell. "They have breached not just one account. They have breached a million accounts in a single stroke." Savvy hackers, he predicts, will soon figure out how to automate the process of stealing IDs -- and then apply for new credit cards online en masse.

That sounds like sales hype, coming from a company that sells products aimed at controlling the problem. But other security notables, such as Bruce Schneier, chief technology officer of Counterpane Internet Security, which sells network-monitoring services, have imagined similar scenarios for one simple reason: Crooks tend to go where the money is.

It might take some catastrophe to force dramatic changes in the way the world approaches Net security. With corporate tech spending spotty, the federal budget deficit soaring, and states and counties in financial distress, chances are slim that a preemptive attack on the violators of Internet security will be launched. The alternative is a war of attrition -- and many more battles ahead to protect the sanctity of the one true worldwide interactive medium.

**Business Week on-line - acesso em 22/9/2003**