numerous interactions with enthusiastic crowds, creating a forum for promoting the importance of their cause. For athletes who have suffered a personal loss, the marathon is an opportunity to convert emotional anguish into a physically challenging fight against a disease. The long hours of team training and race day fans form a social network of invaluable support to DFMC's members. Both fundraising and running a marathon are challenging tasks, yet the two complement each other such that the mission as a whole is more than the sum of its parts.

—Anne van Grondelle

▸ **FROM READERS**

Back to college

Thank you for the article by Claudia Goldin and Lawrence Katz on "The Shaping of Higher Education in the United States and New England" (Q4 2001). The data on public spending and enrollments by state were particularly helpful.

In citing the establishment of private colleges in New England, however, Goldin and Katz did not mention that many were formed by religious groups: Harvard by Congregationalists, Boston University by Methodists, Tufts by Universalists, Holy Cross and Boston College by Jesuits, and Northeastern University and Springfield College from the YMCA movement. In addition, Harvard accepted state appropriations for almost two centuries and was an early prototype of a quasi-public college, designed to provide preachers and teachers for church and state. Economists rarely look at the influence of religion, but even today 40 percent of college freshmen consider "integrating spirituality into my life" as "essential" or "very important," according to a survey undertaken by UCLA and the American Council on Education.

As to whether a philanthropist will ever again have his or her name on a first-rate private college: The Franklin W. Olin College of Engineering, in Needham, Massachusetts, was established after a 1997 gift of $300 million from the foundation created by F.W. Olin, of Olin Industries. It was designed to be both first rate and free. Perhaps it's still early to rule out either Bill Gates or Ted Turner!

Joe Cronin
President of Bentley College, 1991–97
Secretary of Education, Commonwealth of Massachusetts, 1971–75

perspective

Manufacturers should be liable when computer bugs leave consumers in the lurch

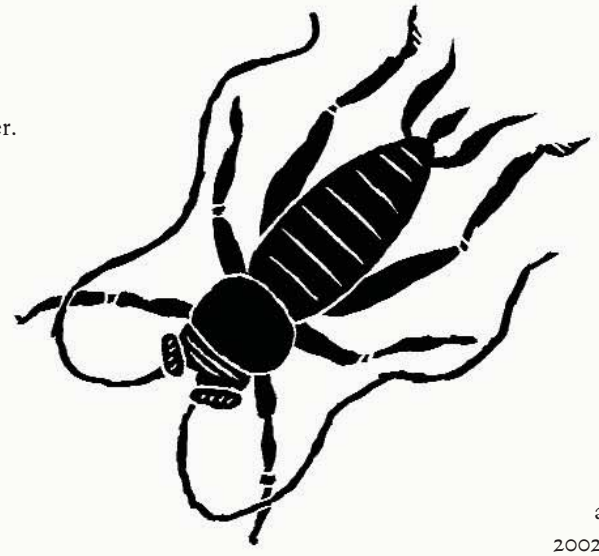
By David Banisar

IN EARLY JUNE, Microsoft announced a serious flaw in a number of its programs—including Internet Explorer, Messenger, and Chat—that could allow a hacker to take control of a user's computer to run programs and access information. This was not the first such announcement by Microsoft this year of a major error in its programs, nor is Microsoft alone in this problem. Every day thousands of computers around the world are disabled or illegally entered because of system and software flaws. At best, these bugs are minor nuisances. But at worst, they open systems to viruses, denial of service attacks, and manipulation by outsiders. The consequences include fraud, release of personal and proprietary information, and loss of business due to downtime. A recent study by the National Institute of Standards and Technology found that software bugs cost the U.S. economy nearly $60 billion each year.

There is no single reason for these problems, but the majority of security holes are due to poor programming and a lack of quality control. Systems and software manufacturers typically place far more emphasis on getting a new system out to market with more profitable features than on ensuring that the system is satisfactorily error-free before it is released. The burden then falls on users to identify and track bugs and fix them before they cause a system failure or are exploited in cyberattacks. There is no other consumer product for which consumers are expected to do so much to ensure product safety, and the creators so little.

THE MISSING INVISIBLE HAND

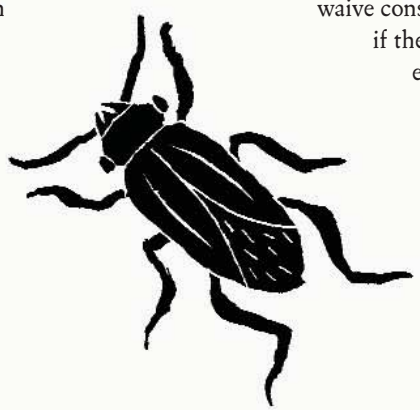
The computer industry's response is that the market should resolve the issue. Users should select software based on its reliability, and the least flawed programs will win. But thus far, market forces have not succeeded in improving software safety. Why? For many types of software, consumers don't have a real choice. Oracle, for instance, controls the market for enterprise database software, with three to four times the market share of its nearest competitors. Recently discovered bugs in its purportedly "unbreakable" latest release, Oracle 9i, did not prevent the company from maintaining this dominance. Its users, especially those with years of data on its system, are so dependent on its products that they have no credible way to threaten Oracle



with shifting to another provider. The result is heightened exposure to bugs and security risks.

Well-functioning markets also depend on the free flow of information to consumers. But instead of keeping consumers apprised about known software flaws, some companies try to hide them. Network Associates, Oracle, Microsoft, and other software manufacturers include provisions in some of their licenses that prohibit criticism of their software without their permission. Some firms even threaten researchers who publish security holes or write program improvements with civil and criminal litigation under copyright law. In one extreme case, a complaint of copyright violations from Adobe Systems led the Justice Department to arrest a Russian programmer who had written a program demonstrating security flaws in Adobe's eBook software.

Law enforcement efforts have not succeeded in discouraging cyberattackers from abusing security flaws. Though entering or disabling someone else's computer has been illegal in the U.S. since 1984, the perpetrators are difficult to identify, and there are serious limits to the help that law enforcement can provide because of lack of resources. Catching the criminals is even more difficult when they lie outside U.S. jurisdiction, as did the Filipino man who caused billions of dollars in damages worldwide by releasing the "ILOVEYOU" virus. Prosecutions are increasing, but there are still only a few hundred each year—nowhere near enough to act as a deterrent.



UNSAFE AT ANY GIGAHERTZ

For nearly 100 years, manufacturers of consumer products have been subject to product liability laws. These laws stipulate that if a reasonable person would foresee that a product would create a risk of serious harm if not carefully made, then the manufacturer is under a duty to exercise reasonable care in the manufacture of the product. If a company sells a product knowing that it is flawed, then even more severe sanctions can be imposed. Manufacturers can also be held liable for products that are inherently dangerous or are foreseeably dangerous. (I'll leave it to readers to make their own opinions about Windows.)

Being held responsible when their products fail has spurred manufacturers in other industries to improve their safety records. Cars, for example, used to be quite insecure, unreliable, and dangerous devices to use. But imposing liability and creating manufacturing standards for cars has greatly improved their safety. Since the first auto safety legislation was passed in the U.S. in 1966, auto fatalities have dropped nearly 75 percent as car manufacturers have started including safety features like seat belts, roll bars, and air bags. In 1991 and again in 2002, the National Academy of Sciences proposed that software and system vendors—like car manufacturers—should be held responsible if they ship programs or equipment without adequately testing for security holes. Yet no action has been taken by policymakers to further this cause. Why must consumers be the electronic crash test dummies for the software companies?

Software manufacturers have worked to absolve themselves of their legal responsibilities by forcing consumers to accept the terms of their licensing agreements at the time of product purchase or installation. These agreements, commonly called "shrink wrap" or "click wrap" contracts, limit or waive consumers' ability to seek damages if the software does not perform as expected—even when the problems are the manufacturer's fault. Not only do consumers not have the opportunity to negotiate these contracts, but in some cases they don't even have the opportunity to read them before committing to the product. (The licensing agreements are often inside shrink wrap and thus inaccessible without opening the box—but most computer stores won't accept opened software for return.) Most software manufacturers also do not provide a warranty, which would allow consumers some recourse if the product did not perform as expected. Many of the licenses go even further, attempting to muzzle criticism. For instance, the licensing agreement for the Gauntlet firewall program, written by software manufacturer Network Associates (NA), prohibited publishing the results of comparative performance tests. When *Network World* magazine printed a negative review of the program, NA threatened to sue them, claiming a breach of the license contract and demanding a retraction.

INSURING A SOLUTION

Fortunately, the tide is starting to turn toward greater consumer protection. Courts and consumer protection agencies are balk-

ILLUSTRATION BY ADAM MCCAULEY

ing at many of the more outrageous provisions in licensing agreements. The New York Attorney General filed suit against Network Associates in February, describing their anti-review provision as a "censorship clause" and asking the court to prevent NA from using it.

Furthermore, the computer industry's effort to get states to enact the model Uniform Computer Information Transactions Act legislation is faltering. The legislation would allow companies to more easily enforce software licensing agreements and limit their liability by removing software as a consumer good subject to the normal consumer laws. But despite the best efforts of software companies and online services, it has been made law in only Maryland and Virginia because of opposition from a variety of organizations, including consumer groups, state attorneys general, computer professional associations, and businesses that buy software.

An important force for change will likely be the insurance market. In July, a federal court ruled that AOL's insurer did not have to cover the costs of a settlement the company struck to settle software problems that prevented thousands of users from getting online. In addition, firms themselves are starting to purchase additional insurance to protect themselves against bugs and cyberattacks, and insurance companies are responding by imposing higher rates on companies using buggy products. One firm already charges 15 percent higher e-commerce premiums to companies using Microsoft's IIS Web hosting platform than those using its competitor, Apache. If this practice spreads, software manufacturers will have to improve their products or risk losing business.

Holding manufacturers liable for software and system flaws will not solve all the security problems. Users will still have to screen for viruses and install firewall software, just as drivers must obey traffic safety laws. But it is time to stop expecting users to pay the price for manufacturers' mistakes. ✳

David Banisar is Visiting Research Fellow at the School of Law, University of Leeds in the United Kingdom. He was previously a fellow at the Kennedy School of Government, Harvard University.

By Alice M. Rivlin ILLUSTRATIONS BY GRADY Mc

Challenges of