

Threat Matrix

A BANK ROBBER. A car thief. A computer nerd. Which is most intimidating?

The bank robber is ominous, but to be honest, he worries me the least. Although there are 8,000 bank robberies every year, I don't have a bank in my house, or even my neighborhood, so I don't feel personally threatened.

The car thief worries me a bit more. I like my car, and more than a million vehicles are stolen every year. And as Craig McCoy reports in the *Philadelphia Inquirer*, car thieves are getting smarter. They're now able to open and start a wide variety of makes and models using illicitly produced "master keys" that even car manufacturers don't possess.

Nevertheless, I'm most troubled by the computer nerd—the type intent on causing malicious mischief on the wonderful Worldwide Web. In the days of Ozzie and Harriet, these nerds might have just made prank phone calls or soaped an occasional window. Now, they playfully design computer viruses with cute names like Bugbear, Blaster, and Swen.

These aren't just simple nuisances. In 2001, the Code Red Internet worm spread to 360,000 computers and cost businesses more than \$2 billion in cleanup costs. Since last summer, the MS Blast worm and the SoBig e-mail virus have spread to more than a million computers. And the Welchia virus recently shut down the State Department's visa-processing center for nine hours.

I recently traveled on business with my laptop. Normally, I work complacently within the protected confines of my company's firewall, but once outside, chaos reigned. Repeated attacks caused recurrent shutdowns, making it virtually impossible to perform the simplest of tasks.

Back at the office, I discovered that my computer lacked the most up-to-date security patches and was triggered to infect the entire company. I felt as if I'd ventured into a disease-ridden neighborhood and returned with a communicable disease. And all I wanted to do was read my e-mail.



According to Wade Roush, senior editor of *Technology Review*, "the Achilles' heel of today's Internet is that it's a system built on trust.... It delivers packets whether they're legitimate or the electronic equivalent of letter bombs."

According to Jack, my IT director, hackers have made it unsafe to operate remotely without increasingly stringent precautions, such as checking both the Microsoft and Symantec security sites to download "system patches" (which Microsoft issues at the rate of more than one a week) at the start of each session.

Things aren't entirely safe at home either. In "Firewall Follies" (*Technology Review*, September 2002), Simpson Garfinkle commented that "firewalls don't make

business systems significantly more secure. And by focusing attention on defending the perimeter rather than defending information assets within an organization, firewalls foster lax internal security practices that magnify the damage that insiders can inflict."

Wow. This sounds more like a strategy for defending Baghdad than conducting business. But the problem is serious. My company has just 300 employees, and we now have three people (more than 1 percent of payroll) devoted to computer security full time.

What's Our Defense?

Tougher programming standards could eliminate security holes caused by poorly written code. As a major software purchaser, the federal government can exert its influence directly, or it could invoke the less subtle option of federal regulation.

There's also the option of expanding product liability law to software vendors. Thus far, vendors have avoided such suits partly by licensing rather than selling their software, and partly through extensive disclaimers. But as users become more frustrated, this could change. A suit was recently filed against Microsoft, alleging that the giant software maker doesn't do enough to inform its users of the scope and seriousness of security breaches, thereby leaving many users open to exploitation.

But my company's IT director may have a better solution. "Bring back public caning," says Jack. Perhaps a good spanking is just what these mischief makers deserve.

The computer nerd, it seems, has moved front and center in our personal threat matrix, and he's not likely to go away anytime soon.

RICHARD T. ZATORSKI IS CHIEF ACTUARY AT THE GUARD INSURANCE GROUP IN WILKES-BARRE, PA.