SIMSON GARFINKEL

THE NET EFFECT

LEAKY CYBER BORDERS

By the time you read this, I should be filthy rich.

I recently received an e-mail that claimed to be from a high-ranking Nigerian official who had discovered some funds stolen by Nigeria's former military government. The bank account holding this money, I read, could be used only to transfer the funds abroad. All I needed to do was respond with the name of my bank, my bank account number and some personal information. In return, "Dr. Ahmed" would wire me 35 percent of the trapped $41 million.

Of course, this junk e-mail was nothing more than an invitation to be swindled. With my bank information, the good doctor could clean out my savings, wiring the money through a series of other accounts so that I would never see it again.

Like me, you probably delete dubious electronic missives like this one without much thought. But apparently, not everyone is so skeptical. Last year, the Nigerian banking swindle made number three on the National Consumers League's top-10 list of Internet scams. The Federal Trade Commission says that Americans are losing more than $100 million a year to international con artists. But things could be much worse: most of the Nigerian scam letters sent through paper mail get stopped and destroyed at the border by the U.S. Postal Service—ironically, because they are sent with counterfeit stamps.

But while the government vigilantly patrols our physical borders, it is doing precious little to control our electronic ones. Consider this: someone trying to bring fresh fruit from Europe into the United States will be stopped by an agent of the U.S. Department of Agriculture. But there's nothing to protect you from the electronic damage wrought by an infected Microsoft Word file sent to you by some computer hacker in Iraq. Many scholars and civil libertarians say that this is as it should be: while controls on physical borders involve the movement of mere people and things, electronic-border control would regulate information and ideas. Any attempt to block the importation of ideas would be, by definition, an exercise of state censorship. And that, many believe, is a no-no.

But an increasing number of the messages that our computers receive each day from overseas do not carry any ideas at all. These e-mailed files contain sequences of data designed to make our computers crash, or worse, to break into our systems so that foreigners can steal secrets and use our computers as bases for attacking still more machines.

Because of this electronic onslaught, I have followed the lead of many businesses and installed a firewall that relies on "military-strength" cryptography. I have electronic locks, alarms and even an automated intrusion detection system. I will defend myself, no matter whether the attack is from the college freshman next door or a hostile government halfway around the world. Organizations that don't implement these kinds of defenses are considered both negligent and stupid.

As a computer programmer, I have enjoyed the challenge of this constant attention to security. (I have profited from it too, through the books I've written on the subject.) But I'm an unusual case. For most businesses, spending on electronic security is like protection money paid to the mob—necessary for survival but not particularly productive.

This thirst for supersafe electronic security is without parallel in the physical world. We don't berate a fabric boutique for not defending its perimeter with the same vigor and prowess as an aircraft carrier floating off enemy shores. That's because the aircraft carrier (and the rest of the U.S. military) *is* the boutique's first line of defense. The boutique relies on the government for much of its border control, and as a result, the security afforded by the store's plate glass window and five-pin locks is usually more than sufficient.

The government won't let you bring fresh fruit from Europe into the country. But there's nothing to protect you from the damage wrought by an infected Microsoft Word file sent by some hacker in Iraq.

And that's probably where the world is headed. Just as nations now regulate their physical frontiers, so too will they regulate their electronic ones—using computer security rather than objectionable ideas as their justification. Already, China and many Middle Eastern countries have installed "national firewalls," blocking access to some U.S. Web sites because of their content. France and Germany may soon do the same, blocking access to neo-Nazi content.

At a computer conference I attended last summer, one speaker held up a sign that showed a block of Internet addresses that were assigned to Asia. The numbers were surrounded by one of those red circle-and-slash marks. The speaker had gotten so tired of the constant probes, attacks and junk e-mail from those addresses that he had simply cut off their access to his computers. "Asia: just say 'no,'" he said. If this mood spreads, Internet service providers might begin to offer geography-based blocking as a value-added service. Or perhaps there will soon be mandatory firewalls against packets that originate in particular countries. After all, why shouldn't those e-mails from overseas be virus-scanned?

A big part of the Internet's magic is the liberation from concern over distance and borders. Last September's terrorist attacks were so devastating, in part, because a group of attackers from halfway around the world reached through our national borders and attacked civilian targets. The same basic thing—not costing lives, but destroying property and wreaking great economic damage—happens every day on the Internet. TR