Stop! Cyberthief!

Technology: Don't be alarmed, but the law can't cope with computer crime

By Michael Meyer

A SUBURBAN MOTHER IN MAMARONECK, N.Y., goes to the shopping mall. She happens upon her 14-year-old daughter in the company of a stranger. She calls the police, who discover that the man is a suspected pedophile from Seattle—and has enticed the girl into a tryst over the family's computer.

A Midwest technology company spends years developing a new product. Before it goes into production, cybercrooks steal the designs. Frustrated executives say the technology was worth "millions if not billions" of dollars.

A group calling itself Victims No More accuses a student in California of being a "date rapist." It posts messages on computer bulletin boards across the country giving his name, address and phone number—and invites readers to "let this rapist . . . know he will pay!" Is it fair warning, or libel?

Such is the brave new world of cybercrime, probably the fastest-growing brand of wrongdoing in America. Out there in the electronic ether, cruising the ubiquitous computer web known as the Internet, bad guys are at it. Lonely cybersickos are stalking women and kids via PC. Digital bandits are defrauding widows, running securities scams, purloining credit cards and hacking government and industrial secrets for fun or profit. Yet for all the horror stories, there's no reason for hysteria. Cybercrime isn't epidemic. It's just that our excitingly new virtual world, accessible with a few strokes at the keyboard, is coming to resemble the real world—with all its diversity and problems. The trouble is, there are few cops on the Net. Laws that bite here often lack teeth there. "It's the Wild West," says a spokeswoman for Prodigy, the burgeoning online information service. "No one owns it. It has no rules."

It's no accident that cybercrime is surging. Everyone, these days, seems to be buying PCs and getting wired. We're paying bills over the Net, flocking to join Prodigy or America Online, morphing from a paper society to a culture of bits and bytes. Everything from personal banking to libraries to confidential medical and business records is being digitized and zapped around the world at the click of a mouse. The rewards are tremendous: new efficiency, greater convenience, information at our fingertips.

But if all that is valuable can be reduced to electronic blips, it's that much easier to abuse or steal. Says André Bacard, author of “The Computer Privacy Handbook”: “Our privacy is an illusion.”

It's hard to gauge the economic effect. “Anyone who tries to put a dollar on the problem is blowing smoke,” says John O'Leary of the Computer Security Institute in San Francisco. Unlike real-world burglaries, say, few electronic crimes are reported. Many are never detected. Yet clearly, businesses are being targeted as never before. Ernst & Young, a leading consulting firm, recently concluded a study of 1,271 companies. Half of them reported financial losses from security breaches and digital thievery over the last two years, up substantially from the past. Yale University reports that hackers try to break into its computer-science system roughly 250 times a month. No one is immune. General Electric not long ago reported that electronic intruders forced it to sever links to the Internet for three days. IBM and Sprint have also experienced intrusions.

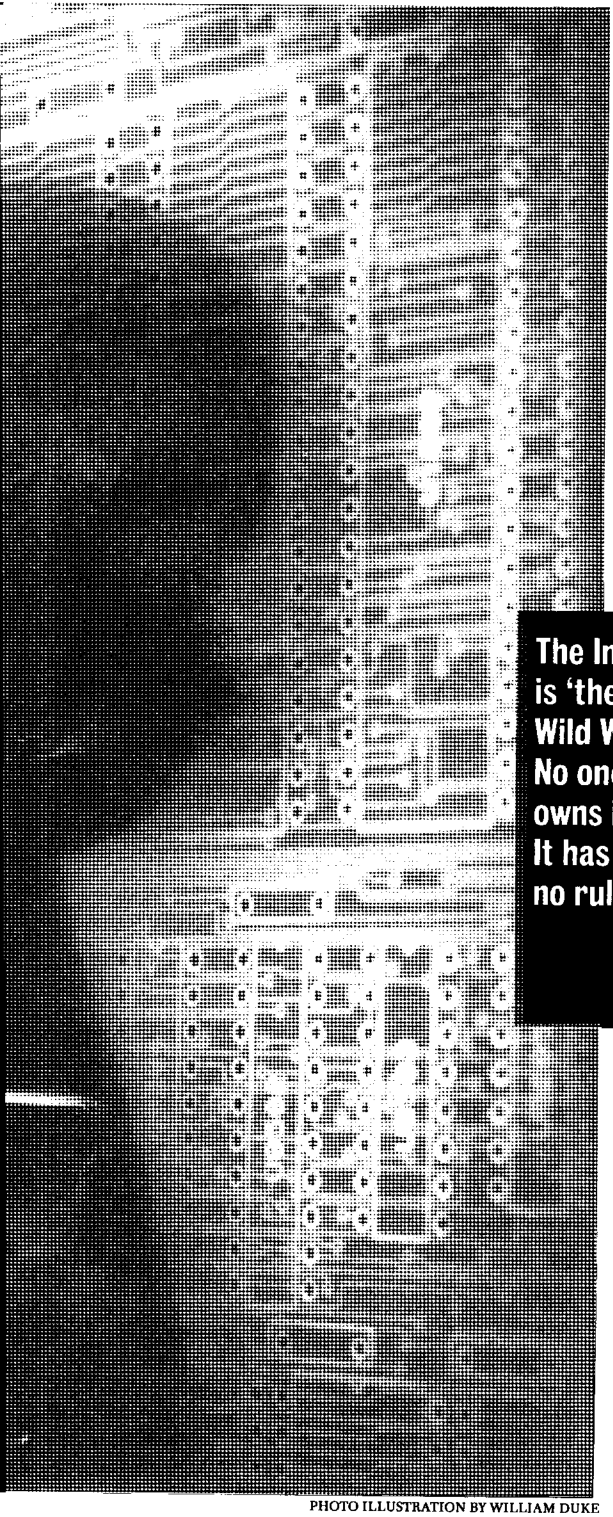


PHOTO ILLUSTRATION BY WILLIAM DUKE

Last week brought word that high-tech crooks have developed a new way of “spoofing” their way into even well-defended computers. The technique involves breaking the code words on one computer in a network, then impersonating the “friendly” machine to bypass the defenses of others. The target was Tsutomu Shimomura, an authority on electronic security at the San Diego Supercomputer Center. At least one thief succeeded in stealing a number of sophisticated programs, some potentially useful in unscrambling cellular-telephone codes. Shimomura fears they could be used to break into yet more computers—not for fun, as most hackers do, but for financial gain (following story).

The Internet is ‘the Wild West. No one owns it. It has no rules.’

Those gains can be huge. Consider the ill-gotten wealth of “Dr. Demonicus.” High-school friends from Marrero, La., remember Dwayne Comeger as a smart, straight-arrow kid whose lack of interest in academics won him, after graduation, a job at a Popeye's fast-food joint. But he had bigger dreams. According to the federal indictment, he gave himself a flashy alias and embarked on a classic computer scam; he would first scan phone directories for the names of lawyers and doctors and such, police charge, then rifle the local credit bureau's computers for confidential information on them—such as credit-card numbers. He and others allegedly used those numbers to buy computer equipment, gold coins and other merchandise, which he would have delivered to vacant houses held by the Department of Housing and Urban Development. Comeger's ring is charged with stealing goods worth $200,000; if convicted, he faces 50 years in jail and a $2.25 million fine.

There's even bigger business in pilfering telephone credit cards. Late last year, in just one case, U.S. investigators broke an international ring of racketeers operating out of Majorca. Abetted by phone-company insiders, they sold 140,000 stolen phone cards over computer bulletin boards in the United States and Europe. Hackers used them to make $140 million in long-distance phone calls—sometimes to pay for their time online, other times to tap into remote computers and download bootleg software. By some estimates, as much as $2 billion in software was illegally copied off the Internet last year, a growing share of the total $7.4 billion the Software Publishers Association guesses was lost to piracy in 1993.

As cybercrooks grow more technologically sophisticated, so will their crimes. A new breed of “crackers” (hackers who have gone criminal) are getting into industrial espionage. A sign of the future: William Malik, research director at the Gartner Group, tells how one of his clients, a large manufacturer in the Northeast, lost a $900 million contract to a rival. Insiders claim the competitor hacked into their computers and discovered the company's bid.

For parents who have recently bought PCs for their kids, there are more important worries. Ask the mother from Mamaroneck, a leafy suburb of New York City, whose daughter was nearly seduced by an accused Info Age pedophile. According to police records, Alan Paul Barlow, 51, began courting the 14-year-old over the Internet last spring, posing as a 13-year-old boy on a bulletin board frequented by young people. As they digitally chatted, over time, he became more and more intimate. He called his sex “Oscar,” hers “love bunny.” They exchanged nude photos. By June, after he confessed to being older, they agreed Bunny and Oscar should meet. The girl found him a motel, he flew out from Seattle. Purely by chance, her mother walked by the Big Top at the local mall on the day of assignation and saw her daughter and 10-year-old son having a soda with Barlow. Police have since discovered he was in computer contact with 20 to 30 young people, from the East Coast to the West Coast and points in between. In Seattle, he has been charged with statutory rape, including several counts of having sex with a minor under the age of 12.

Exxxtasy: The Internet is no haven for sex offenders. But it does make it easier for the Barlows of the world to reach out and touch someone. When kids fall into conversation on a computer bulletin board, their guard is down. They feel safe at home. A contact is made that can end, however infrequently, in ugliness if not even tragedy. Ease of access makes all the difference. A teenager who might be too shy to buy a dirty magazine at a newsstand, say, feels no such inhibitions online. Less than 5 percent of the 55,000-odd bulletin boards on the Net offer X-rated fare. But they're easily found, with names like Exxxtasy Adult.

Says one computer-industry expert: 'Our privacy is an illusion'

What do we do about this kind of crime, be it a case of child pornography or some cyberpunk posting free copies of IBM's latest software? For parents dealing with sex, the lesson is to beware. "Parents should instruct kids never to meet alone with anyone they've encountered online, or respond to sexually explicit e-mail," suggests John McLean, a Massachusetts police officer who tracks electronic sex offenders. That advice might serve just as well for anyone foolish enough to be tempted by, say, one of the myriad cyberscams that have proliferated on the Net. Maybe it's that tip on hot "penny" stocks on investment bulletin boards, or the come-on to entrust your nest egg in Zairean gold futures with that nice virtual broker in Alberta. Whatever the case, shady operators are at work, trying to persuade unsuspecting investors to give them their money. Securities regulators are pretty much powerless to stop such things. When it comes to cybercrime, it's largely up to PC users to keep themselves from becoming victims.

Still, there are things state and federal authorities can do. The main problem is that real-world laws apply badly, if at all, to cyberspace. Many states, for instance, could not prosecute Alan Paul Barlow on criminal charges because statutes usually don't cover electronic communications. More recently, there was the case of a student at the Massachusetts Institute of Technology, accused of letting people post copyrighted software on a bulletin board he operated. When other users downloaded more than $1 million worth of the stuff, U.S. prosecutors charged him with wire fraud. A federal judge dismissed the case in December, almost contemptuously, on the ground that laws crafted during the telegraph era couldn't possibly cope with the abuses of the Information Age.

Clearly, the Internet revolution will force us to rethink how we regulate our world. The Clinton administration proposes tightening federal copyright law to explicitly cover property transmitted on the Net. Business and government agencies are groping their way toward a common encryption standard that would guarantee the security of commercial transactions. Regulators of every stripe are staffing up to monitor their particular lane of the Highway. They've got some catching up to do, but so what? Cybercrooks, in the end, aren't that different from plain old crooks.

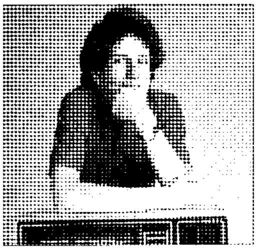
With ANNE UNDERWOOD *in New York,* PATRICIA KING *in San Francisco,* STEVE RHODES *in Chicago and* DEBRA ROSENBERG *in Boston*

THE GREATEST HITS OF HACKING

AP

September 1970

John (Captain Crunch) Draper uses whistle in the cereal box to simulate long-distance-call tones. Arrested repeatedly in the '70s for phone tampering.



MICHAEL VOLLAN

July 1983

FBI busts the '414s'—Neal Patrick and six other Milwaukee teens—for computer trespassing. Patrick gets immunity; others get probation.

JEAN-LOUIS ATLAN–SYGMA

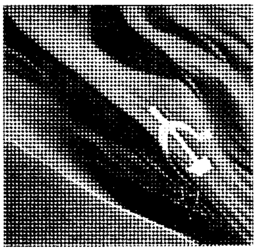
November 1988

A computer virus, known as a worm, cripples the Internet. The culprit, Robert Tappan Morris, is convicted in 1990 and fined $10,000.

VAN NUYS DAILY NEWS

December 1988

Kevin Mitnick, 25, is charged with stealing programs and tapping into Digital Equipment's computer network. He gets a year in jail.



SOVFOTO–EASTFOTO

March 1989

German hackers enter U.S. military computers. Three are charged with spying for the Soviets and sentenced to jail terms, but receive probation.

PHOTOFEST

October 1989

The Friday-the-13th virus is poised to strike. Earlier, it caused turmoil in British computers. Despite fears, reported incidents are minor.

PETER FREED

May 1990

With Operation Sun Devil, Feds seize computers and discs in 14 cities. In response, Lotus's Mitch Kapor forms the Electronic Frontier Foundation.

ROBERT MAASS FOR NEWSWEEK

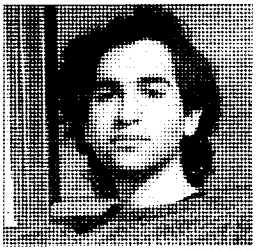
July 1992

Five members of Masters of Deception are indicted for computer break-ins. Mark (Phiber Optik) Abene gets a harsh one-year sentence.

AP

December 1992

After a 17-month manhunt, Kevin Lee Poulsen—alias 'Dark Dante'—is indicted for stealing military documents. The case is pending.



JOHN BLANDING–BOSTON GLOBE

April 1994

MIT student David LaMacchia is indicted for allowing more than $1 million in software to be distributed over the Internet. Charges are dropped.