

Terror's Next Target?

Terror's Next Target? Networks: Critical U.S. information systems are full of holes that could be exploited by attackers living half a world away Vulnerabilities in critical information systems may make them easy targets for future terrorist attacks By Erik Sherman NEWSWEEK Oct. 15 issue — Look past the planes. (Can you?) How about the power grid? Last spring someone broke into the computer systems of the California Independent System Operator (Cal-ISO), the state manager of long-distance electricity transmission. According to Cal-ISO, the target was a test system unconnected to the grid. There was no damage. Still, the electronic intrusion, looked at in the light of the Sept. 11 attacks, unnerves the organization. The word that comes to mind: vulnerability. "Did both incidents reinforce in our minds the need to be vigilant?" asks Gregg Fishman, a Cal-ISO spokesman. "Yes. To take extra precautions? Yes."

CAL-ISO FACES A THREAT that could reach any company: cyberterrorism. Using computers half a world away to attack a country's infrastructure was for years largely a theoretical discussion among security experts. No more.

Evidence of electronic warfare has been insignificant to date. Recent Web-site attacks were the work of individuals. The same goes for Internet viruses. "The most clear-cut example of cyberterrorism we've seen recently is the little war going back and forth between U.S. and Chinese hackers, who have been defacing the Web sites of each other's countries," says Fred Rica, a partner and national-threat-and-vulnerability-assessment leader at consulting firm PricewaterhouseCoopers.

These attacks are simply nuisances—"More cybervandalism than cyberterrorism," says George Kurtz, coauthor of "Hacking Exposed" and CEO of security consultant Foundstone, Inc. But many experts, including Kurtz, are afraid that penny ante may soon be passe. "I look at history to guide where people will go. In a war, one of the

first things people try to take out is manufacturing, oil-refinery plants.”

Utilities, telecommunications plants and factories have always been vulnerable to physical attack. Now they make electronic targets, too. Operators have increasingly managed critical systems at remote locations over the Internet with small computers called process-control devices. The remote operation is a great convenience to communications and energy companies that may have equipment spread over a large distance. But it creates liabilities. “These process-control devices are simple devices that run stripped-down operating systems,” Kurtz says. “No one wants to shut [the factories] down to fix them, but they are vulnerable.”

Even when systems are not connected to the Internet, they may rely on dial-in technologies that, according to Kurtz, give someone with technical savvy a 90 percent chance of breaking in. Interception is difficult; the perpetrators can launch attacks from virtually anywhere in the world. Unlike physical attacks, these provide no hard records, such as hotel reservations or airline tickets, to telegraph a warning.

Transportation facilities are vulnerable, too. An incident in 1997 gave a taste of what might be possible through an electronic attack. A teenager who gained access to a phone switch at the Worcester, Mass., airport accidentally cut all communications for the control tower for six hours. Air-traffic controllers had to direct traffic with one mobile phone and some battery-powered radios. Nothing like that has happened since. Still, a year ago the General Accounting Office issued a report stating that the Federal Aviation Administration’s computer-security program “has serious and pervasive problems.” These included numerous untested air-traffic-control systems and a failure to thoroughly address previous security reviews and recommendations, such as always requiring user passwords and thoroughly tracking known software-security problems. “A vast majority of cyberattacks are never heard about because the victims don’t even know they’ve been broken into.” — AMIT YORAN president, Riptech, Inc.

Many companies are more vulnerable to electronic intrusion than

they realize. “A vast majority of cyberattacks are never heard about because the victims don’t even know they’ve been broken into,” says Amit Yoran, president of security-services company Riptech, Inc., and a former information-security program director at the Department of Defense (DOD). “In some of the studies we’ve done, less than 3 percent of the folks we break into [during an evaluation] even detect us or have any reaction or response to our attacks.”

The actions at Cal-ISO demonstrate that attacks can come from anywhere, which is one of their great dangers. Whoever broke into the power grid’s computers apparently did so from China. But nobody’s sure. With even a basic knowledge of Internet communications, users can muddy their trails, making an action appear to come from another location. “Professionals are going to cover their tracks in such a manner that it takes you a very long time and a lot of manpower hours to track them down,” says Michael Estes, global-security-compliance and monitoring-service manager for defense contractor Computer Sciences Corp.

Some Web sites make it easy for attackers. Richard B. Isaacs, a certified protection professional and senior vice president at the lubrinco Group, an investigative-and-protective-services firm, remembers a former Web site run by the DOD. “They had one place where they had a picture of the base, and as you moved the cursor, it would give you the latitude and longitude of what you were on,” says Isaacs. “It was great not only for amusement value but to save someone the trouble of doing a survey before launching a missile. Why does the DOD have a public Web site? Are they trying to generate more business?” It was only in late September that the National Imagery and Mapping Agency stopped selling highly detailed maps that showed military installations to the public. Some private corporations are even more reckless with information about their own systems. “If you understand how they operate, what their critical information systems are, how they’re wired, you have a better idea of how to attack,” says John Woodward, director of information warfare for MITRE, a nonprofit company providing security consulting to parts of the federal government, including the Pentagon. Sometimes the knowledge is provided piecemeal in news

stories about the company or in case studies provided by product vendors. “Very often you can find information that the IT company publishes in a journal,” Woodward says. “By the time you find all that information and pull it together, you can develop a pretty clear picture of the system they built.”

A number of experts think that electronic attacks will not be the focus of terrorist organizations. “From studying terrorists for 30 years, [I find that] they prefer the destruction to be highly visible,” says Martha Crenshaw, a professor of government at Wesleyan University in Middletown, Conn., and an authority on terrorism. “If it were a choice of blowing something up or something electronic, I think they would go for blowing something up. The images on television, I think, are important to them.”

“The emphasis when people talk of cyberwar is the Hollywood mentality of Travolta in ‘Swordfish’ [a movie about cybercrime],” says Richard Forno, chief technology officer of Shadowlogic LLC, a Dulles, Va., information-assurance firm working with government and national-security clients. “Cutting-edge high tech is the sexy aspect of what they call cyberterrorism.”

But that does not mean that the nation’s infrastructure is safe. “If you have a situation where all of a sudden a critical part of your network or the infrastructure disappeared because of a couple of truck bombs, that’s a different situation,” says Forno.

Physical attacks could also cripple facilities on which the nation’s infrastructure relies. One expert who asked not to be named pointed out that the Internet itself heavily depends on resources concentrated in Virginia, including a major switching point and telecommunications facilities. “Just shut down the power supplies to that area,” said the person. “There are any number of ways you could do it without touching the building.”

There is a danger, however, in companies’ thinking that an electronic attack is a virtual impossibility, because the sense of safety becomes an excuse for sloppy security. “If something is so darn critical, why is it on a public network in the first place?” asks Forno, voicing an

opinion of many in his field. “If something is deemed critical, then you have to give it increased levels of security and attention. We’re at a time now when people have chosen to sacrifice security for convenience.”

In some cases, the answer is to pull the plug. “You cannot get cyberattacked if you are disconnected from the network,” agrees Elad Baron, CEO of Ft. Lee, N.J., security-technology vendor Whale Communication. “It used to be that all those sensitive networks were physically disconnected from the Internet. But we get amazed time and time again. They’re not officially connected to the Internet, but you get an operator who needs access from home and who is also connected to the Internet.”

Electronic security becomes even more critical because, unlike with an attack in the physical world, it is not possible to simply close down all access points to the United States. Given the way systems are set up and software is written, there are also likely to be access points unknown even to a company’s management, like an unguarded border crossing. “It’s just as easy to [attack] from any place, and you cannot shut the Internet away from the rest of the world,” Baron adds.

Making the nation’s infrastructure safer is not an overwhelming and impossible task. “You have a finite list of resources that need to be protected: all the utilities, electricity, gas, nuclear plants, military sites,” says Baron. “You don’t need to protect every house connected to the Internet.” Removing dial-in communications, disconnecting systems from the Internet and adding intrusion-detection software are common steps. But enforcing security will take some political and financial will. “You have to have some government regulation over this,” says Baron. “You can’t just trust the private sector. People might say this is a violation of capitalism, but terrorists don’t follow the rules of capitalism and democracy.”

After hearing and ignoring warnings about computer security for years, the private sector now seems ready to cooperate. “It’s not on the back burner,” says Kurtz. “I spoke to one client today who said, ‘Anything that has the word security in it is basically going to get

pushed through’.”

The atmosphere seems the same on Capitol Hill. The Department of Justice and Congress have been working on variations of an antiterrorism bill that would make many types of currently criminal computer activities even more serious. Those found to be coercing the government or retaliating against its actions would be guilty of federal terrorism. Under the measures being considered, a judge would have the option to order a jail sentence of any length, up to and including life. The bill being recommended by the House Judiciary Committee uses this language. On the Senate side, a spokesman for Patrick Leahy, chairman of the Senate Judiciary Committee, says the senator is in agreement with the Department of Justice “as far as cyber issues are concerned.”

Will Congress go too far? “This is way overbroad,” says Shari Steele, executive director of the Electronic Frontier Foundation. “They may catch terrorists in their net, but they’re catching others, too.” Steele offers an example of an irate taxpayer who defaces the Internal Revenue Service Web site. Such an action would qualify as a federal terrorism act. “That’s criminal behavior, and you should be prosecuted for that, but it’s not terrorism, and we have to be careful because the punishment [can be] so high.”

As Mick Jagger almost said: You can’t always get what you want. But if you do, you just might find you get more than you need.