

from ITwhitepapers.com

ITwhitepapers

Search our library

Who Are My Best Customers? Get Greater Value From...

This paper will focus on how a company might identify its best customers, but the same process could be used for other...

NAC at the Endpoint: Control Your Network Through...

Protecting IT networks used to be a straightforward case of encircling computers and servers with a firewall and...

COMPUTERWORLD

Government



Print Article



Close Window

The new ground zero in Internet warfare

The power grid is an obvious target for terrorists, but experts disagree about how to secure it

Julia King

April 27, 2009 ([Computerworld](#)) When it comes to critical national infrastructure, the highly distributed and ultra-interconnected U.S. power grid is, hands down, the most vulnerable to cyberattack. On this one point, many cybersecurity experts seem to agree.

Yet just how likely a terrorist target is the grid? And what's the best way to secure and protect the massive inventory of generators, power plants and transmission lines plus the cat's cradle of computer networks that make up the electric power system?

Talk to 10 experts, and you'll likely get 10 different answers.

"The problem is that we have a hard time assessing risk," says Jim Lewis, a senior fellow specializing in cybersecurity at the [Center for Strategic and International Studies](#). "We seem to settle on either indifference or a Bruce Willis movie."

Up until about a decade ago, things were a lot simpler. The industrial control systems that manage the generation and flow of power were pretty much protected from intrusion by their closed-loop architecture. These control systems existed and operated in isolation from everything else.

But increasingly, these systems have been linked to countless corporate networks for everything from real-time monitoring of electricity generation and transmission to remote meter reading and automated grid operations.

"We had an explosion in business network technology, and as that occurred, individuals in accounting, for example, wanted real-time information at their desktop computers so they could do projection planning," says Michael Assante, chief information security officer at [North American Electric Reliability Corp.](#) (NERC), an industry organization of U.S. electrical grid operators.

The smart grid relies heavily on public communication networks, including cellular networks and WiMax, to digitally monitor and control the grid for more efficient operation, he explains.

More vulnerability

But more connections mean more points of vulnerability, and that's what worries Sami Saydjari, president of [Cyber Defense Agency](#), a privately held security consulting firm headquartered in Wisconsin Rapids, Wis.

"The power grid is controlled by systems that are antiquated and highly vulnerable because they have very little security. They've been historically protected by disconnection," he says.

But the rush to improve convenience and efficiency by tying together administrative systems and billing

The new Quad-Core
AMD Opteron™ processor.
See the power savings in action.

IDG ACCELERATE

AMD

systems over the Internet has created gateways to the power grid control systems, Saydjari notes.



The power grid is controlled by systems that are antiquated and highly vulnerable because they have very little security.

Sami Saydjari, president, Cyber Defense Agency

"The concern that many of us have is that an adversary can jump that gap directly or indirectly and exploit vulnerabilities," he says.

In particular, they could use these control systems to destroy physical things, like generators, or overload transformers and destroy them, Saydjari says. If that were to happen, it could take six months to replace transformers or generators, "and we have no [replacement] manufacturing capabilities in the U.S.," he says. "Germany, China and Japan are our sources."

The exact scenario Saydjari describes actually happened last March in Baxley, Ga. The Hatch Nuclear Power Plant was forced to shut down for two days following a glitch that occurred after a software update was installed on a computer on the facility's business network. When the updated computer rebooted, [according to published reports](#), it reset the data on the control system but also caused the system to misinterpret dropped data as a drop in water reservoirs that cool the plant's radioactive nuclear fuel rods. The plant's safety systems then triggered a shutdown.

Industry officials readily acknowledge that it's indeed possible to break into the control systems via the Internet and cause damage. But surprisingly, they also contend that it's highly improbable that a cyber criminal or terrorist would target the electric grid.

"The average attacker is trying to gain financially from illicit activity," says NERC's Assante. This, he says, explains the far more frequent attacks on financial institutions and e-commerce operations. Power systems, by contrast, "aren't a good place for a cyber criminal to monetize their efforts," he says.

Terrorists generally "want to do things cheaply and quickly," says another industry official who requested anonymity. To figure out how individual electric companies protect their portion of the grid and how they're connected into regional operations would require "a lot of time, money and hard science. From a terrorism standpoint, it's far more likely that they'd drive a truck into a generation station or shoot guns at a nuclear facility."

But Saydjari maintains that a terrorist attack on the power grid would do catastrophic damage. He estimates that such an attack would require about a half-billion dollars and three years to execute, "but this is well within the means of terrorist groups," he adds.

"Some studies indicate that a concerted strategic attack could bring down 70% of the power grid for six months or more," he says. "This would be devastating to the country. Just think about what happened during Hurricane Katrina. When you take away power from a region, civilization degrades. During Katrina, we had a Third World country in some ways. If you multiply that 100 times or more for six months, it's a sovereignty-challenging event."

And meanwhile, less obtrusive cybersnooping is another concern. Earlier this month when *The Wall Street Journal* reported that Chinese and Russian adversaries are regularly hacking the U.S. power grid and seeding it with electronic time bombs, John Bumgarner was not in the least bit surprised.

"It's a known fact that our critical infrastructures are being probed and penetrated by adversaries on a regular basis. Every day, a critical infrastructure in the U.S. is probed by somebody," says Bumgarner, director of research at the [U.S. Cyber Consequences Unit](#), an independent nonprofit security research organization.

Standardizing security

So what's being done to protect the grid? Following a [General Accounting Office report on security weaknesses at the Tennessee Valley Authority](#), the nation's largest public power company, the Federal Energy Regulatory Commission (FERC), in January 2008 approved [eight mandatory reliability standards](#) that NERC developed to protect bulk power systems against disruptions from cyberattacks.

Electric utilities must comply with these so-called CIPS - short for critical infrastructure protection standards - several of which specifically focus on cybersecurity.

"Standards lay the foundation [for cybersecurity]," says Assante. "What makes the power system unique is that it is so interconnected. From a security context, there's the weakest link argument. That's why we have to have everyone doing the same thing."

Prior to 2005, electric utilities were self-regulating, checking up on one another's compliance with NERC-sanctioned security recommendations. Now, however, violations of the mandatory reliability standards approved by FERC carry fines of up to \$1 million per incident per day. "There are some very serious teeth,"

says Assante.

Still, the current regulatory environment has its share of critics, including Joe Weiss, a control systems engineer and managing partner at [Applied Control Systems](#) in Cupertino, Calif.

FERC's jurisdiction covers only the bulk power grid, which includes federal entities such as the Tennessee Valley Authority, Weiss says. Individual states and NERC share jurisdiction over power distribution, and NERC's regulations simply don't adequately address control systems, Weiss says.

For example, "The NERC CIPs wouldn't have prevented incidents that have already occurred," he says, noting that even though the Hatch nuclear facility was shut down for two days last year, it did not violate any of NERC's IT security policies.



Obama is our e-president. He understands technology.
John Bumgarner, director of research, U.S. Cyber Consequences Unit

Looking ahead, industry officials and security experts alike expect the Obama administration to take a much more proactive role in developing and enforcing infrastructure security policy. Those policies will be aimed at defending against cyberconflicts, which can cover everything from attacking the power grid to "network operations, intelligence-gathering capabilities, a terrorist operation and so-called hacktivism, where a group gets together to take down the BBC or CNN," says Bumgarner.

"The Obama administration is going to be doing a lot with cyber-type activities," Bumgarner says. "Obama is our e-president. He understands technology."

Next: [Russia's cyber blockade of Georgia worked. Could it happen here?](#)

Related Stories

- [Internet Warfare: Are we focusing on the wrong things?](#)
- [The fog of \(cyber\) war](#)
- [A short history of hacks, worms and cyberterror](#)
- [Software: The eternal battlefield in the unending cyberwars](#)
- [The grid: The new ground zero in Internet warfare](#)
- [Russia's cyber blockade of Georgia worked. Could it happen here?](#)
- [Cyberwar's first casualty: Your privacy](#)
- [The Internet is down. What does that really mean?](#)