Bracing For a Big Power Grid Attack: 'One Is Too Many'

Part of the nation's power grid is struck by a cyber or physical attack nearly once every four days. Some experts fear the rash of smaller-scale incidents may point to broader security problems with potentially devastating consequences. VPC

Steve Reilly, USA Today
2:18 p.m. EDT March 24, 2015

(Photo: The Indianapolis Star)

About once every four days, part of the nation's power grid — a system whose failure could leave millions in the dark — is struck by a cyber or physical attack, a USA TODAY analysis of federal energy records finds.

Although the repeated security breaches have never resulted in the type of cascading outage that swept across the Northeast in 2003, they have sharpened concerns about vulnerabilities in the electric system.

A widespread outage lasting even a few days could disable devices ranging from ATMs to cellphones to traffic lights, and could threaten lives if heating, air conditioning and health care systems exhaust their backup power supplies.

Some experts and officials fear the rash of smaller-scale incidents may point to broader security problems, raising questions about what can be done to safeguard the electrical grid from an attack that could leave millions without power for days or weeks, with potentially devastating consequences.

> "It's one of those things: One is too many, so that's why we have to pay attention," said Federal Energy Regulatory Commission Chairman Cheryl LaFleur. "The threats continue to evolve, and we have to continue to evolve as well."

An examination by USA TODAY in collaboration with more than 10 Gannett newspapers and TV stations across the country, and drawing on thousands of pages of government records, federal energy data and a survey of more than 50 electric utilities, finds:

- More often than once a week, the physical and computerized security mechanisms intended to protect Americans from widespread power outages are affected by attacks, with less severe cyberattacks happening even more often.
- Transformers and other critical equipment often sit in plain view, protected only by chain-link fencing and a few security cameras.
- Suspects have never been identified in connection with many of the 300-plus attacks on electrical infrastructure since 2011.
- An organization funded by the power industry writes and enforces the industry's own guidelines for security, and decreased the number of security penalties it issued by 30% from 2013 to 2014, leading to questions about oversight.

Jon Wellinghoff, former chairman of the Federal Energy Regulatory Commission, said the power grid is currently "too susceptible to a cascading outage" because of its reliance on a small number of critical substations and other physical equipment.

USA Today, ***"When the Lights Go Out"***
http://www.usatoday.com/story/news/2015/03/24/powergridblackout/24963123/

Because the nation's electrical grid operates as an interdependent network, the failure of any one element requires energy to be drawn from other areas. If multiple parts fail at the same time, there is the potential for a cascading effect that could leave millions in the darks for days, weeks or longer.

"Those critical nodes can, in fact, be attacked in one way or another," Wellinghoff said. "You have a very vulnerable system that will continue to be vulnerable until we figure out a way to break it out into more distributed systems."

'A GAME CHANGER'

Some of the worst fears of those in charge of the power grid's security came true shortly before 1 a.m. on April 16, 2013, when unknown attackers unleashed a coordinated attack on Pacific Gas & Electric's Metcalf substation in northern California.

The attackers severed six underground fiber-optic lines before firing more than 100 rounds of ammunition at the substation's transformers, causing more than $15 million in damage.

The intentional act of sabotage, likely involving more than one gunman, was unlike any previous attack on the nation's grid in its scale and sophistication.

Yet officers did not begin investigating the scene until hours after the shooting took place. Security footage from the shooting is grainy. The attackers were never caught.

Power was not lost, but the nature of the Metcalf attack sent shock waves through the industry.

"Shooting at substations, unfortunately, is not uncommon," Sue Kelly, president and CEO of the American Public Power Association, an industry group, said of the incident at a Senate hearing last year. "But this incident demonstrated a level of sophistication not previously seen in our sector."

At a California Public Utilities Commission meeting last year to review the incident, PG&E senior director of substations Ken Wells said the Metcalf attack was "a game changer."

"No doubt about it, ...this event caused us and the entire industry to take a new and closer look at our critical facilities and what we can do to protect them," Wells said.

USA Today, ***"Power Grid Security Fears Surge Since 2003 Blackout"***
http://www.usatoday.com/story/news/2015/03/24/power-grid-security-solutions-and-ideas-arose-after-2003-blackout/24892721/

Following the attack, FERC directed the industry to write new rules for physical security. The rules, finalized in November, require utilities to identify critical infrastructure that could be vulnerable to attack and come up with security plans. But the new policy drew concern because it does not give FERC authority to independently choose which facilities are critical, leaving the decisions in the hand of industry.

Wellinghoff said while he is glad the new policy is in place, the lack of authority for FERC "could be a loophole that could miss some aspects of the utility infrastructure that are critical."

Also as a result of the Metcalf incident, PG&E said it would invest $100 million over three years on new security around many of its critical facilities, including better security cameras, fencing and lighting.

Yet records from hundreds of other attacks in recent years show similar weaknesses still exist at thousands of electric facilities across the country, allowing repeated breaches.

'SO BADLY BROKEN'

Between 2011 and 2014, electric utilities reported 362 physical and cyberattacks that caused outages or other power disturbances to the U.S. Department of Energy. Of those, 14 were cyberattacks and the rest were physical in nature.

Among the incidents:

- In 2011, an intruder gained access to a critical hydro-electric converter station in Vermont by smashing a lock on a door.
- In 2013, a gunman fired multiple shots at a gas turbine power plant along the Missouri-Kansas border.
- Also in 2013, four bullets fired from a highway struck a power substation outside Colorado Springs.

No suspects were apprehended in those three incidents. Federal data show such attacks are not rare within the sprawling, interdependent network of transformers, power lines and other equipment that make up the electrical grid.

Often, such incidents are shrugged off by the local police who initially investigate.

In March 2013, security officers at the Jacksonville Electric Authority in Florida noticed a man climbing a fence surrounding St. Johns River Power Park, which produces energy for 250,000 northern Florida households.

The man fled when approached, Jacksonville Electric Authority spokeswoman Gerri Boyce said, and was later observed trying to enter a second facility. He fled again and was never caught.

Nobody filed a police report, according to Jacksonville Sheriff's Office documents.

SMALL COMMUNITIES AT RISK TOO

Federal records show it is not just large communities that are at risk of attack. Even small, rural utility companies have been subject to foul play.

After a 2011 cyberattack struck the Pedernales Electric Cooperative — a non-profit utility that serves about 200,000 customers across a vast agrarian region of Texas — the utility's CEO, R.B. Sloan, shared his surprise with the utility's board of directors.

"You would think if they really wanted to have an impact, they would go for something (else)," he said in a public meeting. Sloan said at the time that the utility filed reports with the Department of Energy and FBI, but he was concerned about the way they handled it.

"It's obvious to us that some of the regulatory bodies are not well-equipped to accept these and follow up," he said during the 2011 meeting. "I think this event has made that very apparent."

Now an executive for a Georgia utility software company, Sloan declined to discuss the attack.

While the Department of Energy received only 14 reports of cyberattacks from utilities over the past four years, other reporting systems show rising cyberthreats.

The branch of the Department of Homeland Security that monitors cyberthreats received reports of 151 "cyber incidents" related to the energy industry in 2013 — up from 111 in 2012 and 31 in 2011. It is uncertain whether the increase is due to more incidents or an increase in reporting.

Scott Aaronson, senior director of national security for the Edison Electric Institute, a Washington, D.C., group representing electric utilities, said it's difficult to draw trends from figures reported by utilities because of loose definitions of what constitutes a cyber incident.

"Whether it's 13, dozens, thousands — it's been more art than science to identify what an attack is," he said. "There are probes that happen all the time. Adversaries are essentially looking for weaknesses in a network. I've heard people say millions (of attacks occur) a day."

Aaronson noted that there has never been a successful attempt to cause a power outage through a cyberattack in the United States.

Nevertheless, the interconnected nature of the grid and its reliance on communications protocols that predate modern cybersecurity problems are considered cause for concern by security experts. A simulated cyberattack conducted by the U.S. Department of Energy's Idaho National Laboratory in 2007 exploited a vulnerability at the facility by altering the timing of a diesel generator's circuit breakers, causing thick smoke to rise from the plant.

To prevent such attacks, some critical elements of the electricity industry's infrastructure are completely disconnected from the Internet to keep them insulated from adversaries. The power industry also employs stronger cyberdefense mechanisms than, for instance, the retail industry, which has suffered a string of high-profile cyber intrusions in recent years.

For some industry watchers, physical threats to the grid loom larger. But to experts and officials, each reported attack is worrisome.

Former energy security regulator Josh Axelrod, speaking at a 2013 security conference in Louisville, described a "seven bullets theory" of how a mass outage could be triggered by a physical attack targeting key pieces of equipment.

The Eastern power grid is highly interconnected and relies on rolling power between different utilities, he said, according to a video of the presentation.

"If you know where to disable certain transformers, you can cause enough frequency and voltage fluctuation in order to disable the grid and cause cascading outages," said Axelrod, who now heads the power and utilities information security practice at Ernst & Young. "You can pick up a hunting rifle at your local sporting goods store ... and go do what you need to do."

Thomas Popik, president of the Foundation for Resilient Societies, a Nashua, N.H.-based advocacy group, argued the power industry is given too much leeway to control its own security rules.

"The system is so badly broken," Popik said. "For physical protection, the standards are very weak." PENALTIES DECREASING

Under guidelines set by the Energy Policy Act of 2005, an industry-funded non-profit – the North American Electrical Reliability Corporation, or NERC — writes standards for the industry, which

are then approved or disapproved by FERC, the federal agency that has jurisdiction over the power grid.

In a 2012 report, the non-partisan Congressional Research Service called the regulatory arrangement unusual and said it "may potentially be a conflict of interest" for an industry to write its own rules.

Federal regulators also look to NERC for enforcement of those rules, which has decreased in recent years.

The number of enforcement actions taken by NERC against utilities for failing to follow critical infrastructure protection guidelines decreased 30% from 1,230 in 2013 to 860 in 2014.

After issuing more than $5 million in penalties for critical infrastructure violations in 2013, the organization's figures show NERC issued less than $4 million in such penalties last year.

NERC president and CEO Gerry Cauley said decreasing fines point to increased compliance, rather than decreasing enforcement.

"Longer term, you expect people to get the message and make the adjustments to keep improving," he said. "It's not because we're being nicer."

NERC, along with industry funded groups like the Edison Electric Institute, have also fought legislation including the Grid Reliability and Infrastructure Defense Act, or GRID Act, that would eliminate the industry's self-regulation. Congressional lobbying disclosure records show industry-funded groups spent millions lobbying about the GRID Act since 2010.

Cauley said the industry's technical expertise is essential to ensuring reliability of the system, and legislation lessening the industry's oversight role would be "detrimental."

"The people who run and manage and design the system have to be at the table there to figure out how it should work," he said. "We wouldn't want to lose that. I think we would actually take a step backward if we did that."

Read or Share this story: http://usat.ly/1bqrKaZ