E&E NEWS
Essential news for energy and environment professionals

Gadfly advocates win a round on cyberattack rules

By Peter Behr and Blake Sobczak

Thomas Popik and other principals of the Foundation for Resilient Societies could meet around a kitchen table in Popik's Nashua, N.H., hometown. But diminutive or not, the foundation didn't hesitate to take on the entire electric power industry over the disclosure of cybersecurity hacks against the sector. A few days before Christmas, it was rewarded with a surprising if partial win.

Acting on the foundation's petition, the Federal Energy Regulatory Commission announced a proposed rule that would require companies it regulates to report hackers' attempts to plant surveillance and infiltration software inside grid systems. FERC's current cyber rules require companies to report only those hacking attacks that do damage.

ENERGYWIRE

"We're very pleased," said Popik, an entrepreneur with an engineering degree from the Massachusetts Institute of Technology and a Master of Business Administration from Harvard Business School. He co-founded the foundation after attending what he said was an alarming 2010 briefing at the U.S. Army War College in Carlisle, Pa., on potential grid attacks. He has also helped start several nonprofit organizations, including the Academy for Science and Design, a New Hampshire charter high school for science and math education.

"It's one slice, not even half a loaf," Popik added in an interview. "The need for better cybersecurity reporting has been obvious for more than a year and should have been expeditiously addressed."

"But it's an improvement nonetheless," he said. "I think it's significant that a petition from a citizens group was taken seriously. That's certainly unusual if not unprecedented."

Confining reporting requirements to attacks that actually affect the grid has not kept up with tactics of Russian and other sophisticated hackers, government officials and cyber experts agree.

In October, the Department of Homeland Security issued an unusual alert, warning about a "multi-stage intrusion campaign" beginning last May if not earlier. It didn't name perpetrators but said they were attempting to penetrate nuclear power plants, water systems and energy companies. These were not immediate takedown attacks, but rather attempts to secretly add malware that could be used to steal credentials, plant hidden cyber weapons and open paths for future attacks.

The foundation's petition quoted congressional testimony in 2014 by Adm. Michael Rogers, head of the U.S. Cyber Command, who said, "Foreign cyber actors are probing Americans' critical infrastructure networks and in some cases have gained access to those control systems. This malware can be used to shut down vital infrastructure like oil and gas pipelines, power transmission grids, and water distribution and filtration system."

Following the letter of the rules, however, U.S. utilities reported no actual "attacks" in 2015 and 2016, suggesting a gap in the process, FERC said. The grid's security monitor, the North American Electric Reliability Corp., agreed in a report last year, saying the current "mandatory reporting process does not create an accurate picture of cyber security risk since most of the cyber threats detected by the electricity industry manifest themselves in … email, websites, smart phone applications."

If the Dec. 21 proposed rule takes effect, regulated grid companies would have to report cyber "break-in" attempts, as well, to the electric power industry's online threat portal. FERC will take comments on the proposal for two months.

The "rest of the loaf" that the foundation did not get was its push on FERC to tighten mandatory cyber defense directives on generators and transmission companies with more explicit rules on malware detection, countermeasures and removal.

A coalition of industry trade groups — the American Public Power Association, Edison Electric Institute, Electricity Consumers Resource Council, Electric Power Supply Association, Large Public Power Council, National Rural Electric Cooperative Association and Transmission Access Policy Study Group — urged FERC not to act on the foundation's petition. The issues the foundation raised either are adequately covered by the existing cyber rules or are being addressed in ongoing standards development projects within NERC, the groups said. A bank's computer system can be cyber scrubbed over a weekend; not so a utility's nonstop power delivery, industry experts say.

While it supported a change in reporting, FERC didn't include the foundation's request for tougher cyber defenses in the proposed rule.

Seat at the table

The stream of petitions and research coming from the foundation and its consul-

tants has won Popik and colleagues a seat at the table before FERC and congressional committees. Its research budget draws on contributions, the largest of which, $456,040, came in 2015, according to the group's tax return that year. Popik said the foundation does not publicly identify its donors.

Much of its advocacy has attempted to get FERC and Congress to toughen grid defenses against a high-altitude nuclear explosion, which would release a series of electromagnetic pulse (EMP) waves that would cause multistate blackouts across the United States, according to the latest research findings, and potentially damage high-voltage transformers. That second impact remains hotly contested by Popik's team and grid industry experts.

The foundation's board includes George Baker, a professor emeritus at James Madison University, who led the Defense Nuclear Agency's EMP program, and Henry "Hank" Cooper, former director of the Strategic Defense Initiative Organization and President Reagan's chief negotiator at the Geneva defense and space talks.

Popik sees existential threats to the United States from an EMP attack, a century-level solar flare or a concerted cyberattack. So while sitting at the table, he doesn't hesitate to rattle the china with hard accusations directed at the power industry.

Under a process set down by Congress in 2005, FERC — the federal regulator — cannot dictate rules like the Critical Infrastructure Protection (CIP) cyber regulations. Instead, it orders NERC to craft language to meet its requirements. The writing is assigned to committees of industry representatives whose draft language is put to a vote by grid companies. If it passes, a rule goes back to FERC, which can accept it, deny it or send it back for revision, but not rewrite it itself.

Popik said this process produces inadequate rules. "The way the [reporting] standard was crafted, without a disruption to the bulk power system, no reporting need take place. That is a very high bar," he said. He contended that the defenses against a massive solar storm "have been carefully crafted to have zero impact on electric utilities."

Current CIP rules include a requirement that grid companies "deploy methods to detect, deter, or prevent malicious code, and mitigate the threat of detected malicious code."

"It doesn't say they have to remove the code," Popik said.

Detecting malware

Ted Gutierrez, an expert on utility control system defenses at the SANS Institute, a leading cyber training organization, said the proposed reporting rules are needed. "I fully support this position and believe that there would be significant benefit from sharing information about non-impacting incidents that could lead to early identification of campaigns," he said in an email.

Agreeing with Gutierrez, SANS Director of Industrials and Infrastructure Michael Assante recommended that FERC should prioritize potentially affecting incidents rather than only attacks.

Another expert, not cleared to speak on the record on the issue, noted several "sticking points." "We can't assume all, or most, or in some cases any of the regulated entities have the ability to detect the more sophisticated intrusions," he said. "If you accept that, then how can they be reported or be compelled to report a lurking intruder they've yet [to] and may never detect? That's a tough topic to craft helpful policy on."

He added: "Detected malware has to be removed and removed expeditiously. It may be or may not be what you think it is."

Gutierrez said that the foundation's statement that grid facilities' electronic perimeters are open to attack "is [an] overstatement and exaggerates the risks." While there are some vulnerabilities, he said, "there is no blanket right answer and the determination as to what technologies to implement must be left" to the regulated grid operator.

"As for the suggestion to require the removal of identified malware, I believe that this decision is best left to the [operator] to determine," but operators should explain what they have done, and why, he added.

Tom Alrich, a consultant who closely follows FERC's cyber regulations, said he supports the foundation's petition on expanding reporting requirements. "They were obviously right on this part. People are concerned that there are these attempts to get in," he said.

"The rest of the petition isn't tenable," Alrich said. "The idea that there is all this malware on the network and the companies aren't doing anything about it is kind of ridiculous. They have every incentive to do something about it."

Patrick Miller, managing partner at Archer Energy Solutions, told E&E News that a situation where zero cyber incidents are reported makes no sense. "Given the fact that the industry's probably one of the biggest targets possible from an infrastructure perspective," he said, "I find it hard to believe that there's been literally nothing that would have been of interest" to grid regulators at FERC.

Asked whether utilities would be likely to remove malware on their own, without a specific requirement to do so, Miller said, "I've been to too many generation plants that still have Conficker running around in them," referring to a 9-year-old virus that attacks Microsoft operating systems. "If it's not impacting operations, they don't care, because the effort to take the systems offline to remove [the malware] is an outage, downtime, impact.

"It's important to get rid of malware in the environment. Maybe today it's not causing impact, but maybe tomorrow it is."

Still, he noted that mandating removal is a complex issue — there has to be some way to compensate utilities for potential downtime to remove malware, and a phase-in period would be required for any new binding regulations.

Delay is built into the process, by design, Popik contended in an interview, taking another bite at the industry. The reporting requirement "has been thrown back to the industry for them to make a modification to the standard," Popik said. "They may do that, but it may not be a prudent level of reporting."

"All of this will be a very time-consuming process, which could be years. In the meantime, there would be hundreds or thousands of cyber incidents which are not reported, leaving American society vulnerable" to a cyberattack and blackout, he said.