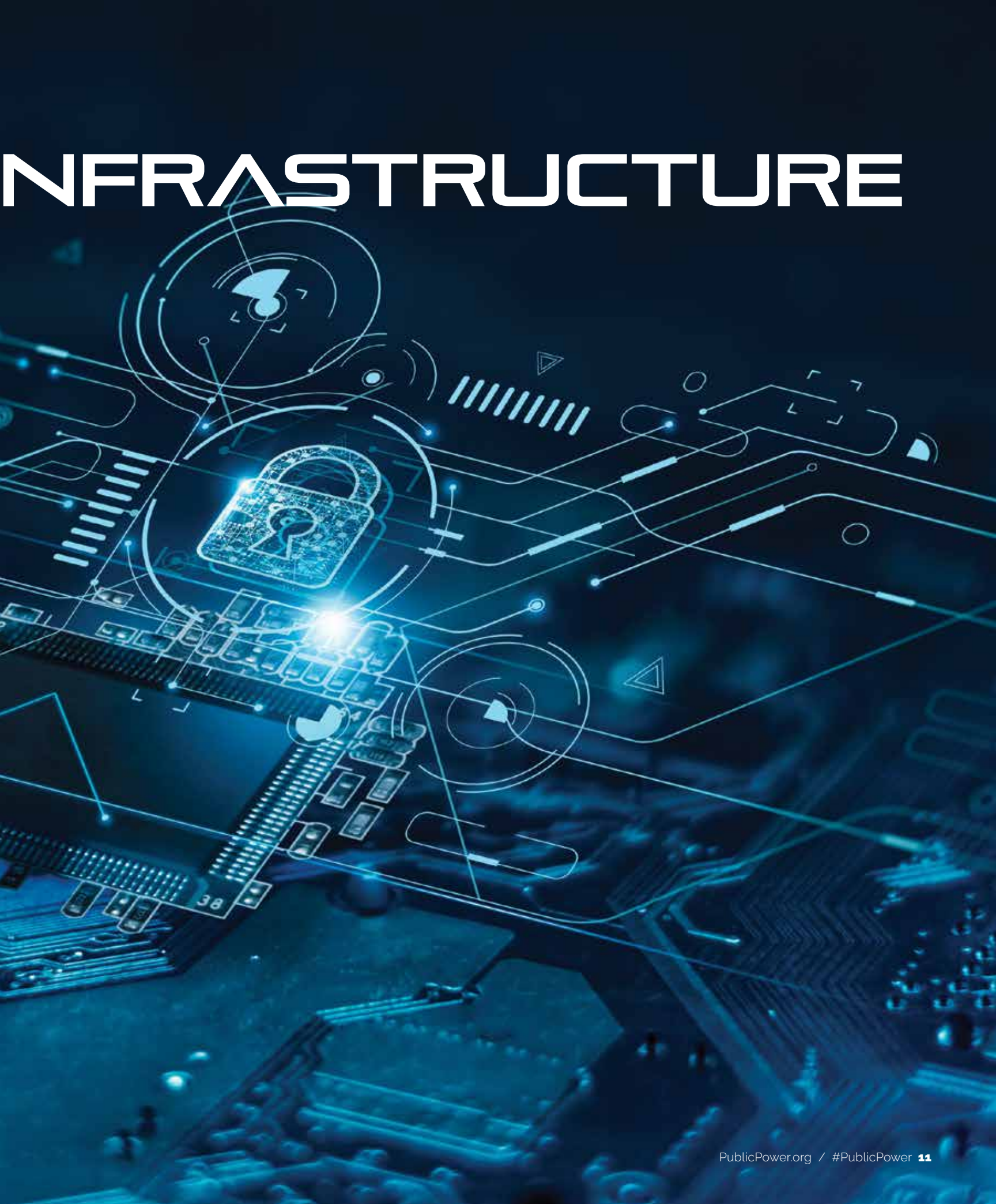
CYBERSECURITY I

Adding sensors, sharing data, greater collaboration, and joint action are all keys to strengthening grid security

BY BETSY LOEFF, CONTRIBUTING WRITER

You cannot fix a problem you do not see, which is why there is a full-throttle drive toward more sensors to monitor the operational technology (OT) that keeps power systems running. There also are a few impediments hampering widespread sensor deployment. Among them are costs and technological know-how. No utility can tackle these issues alone. It will take an industrywide effort to overcome them.

NFRASTRUCTURE



Sensors are vital to the security of the grid. "If you lose your information technology (IT) systems, your operations technology may still run," said Bridgette Bourge, senior director of cybersecurity for the American Public Power Association. "But if you lose your OT, you're offline. Your community is offline."

A successful attack on the electric sector has never happened in the United States, Bourge said. Still, given the current geopolitical environment, "government, private industry, and utilities are on war footing," said Richard Condello, APPA utility cybersecurity deployment manager. "Everyone is hypervigilant, and it's escalated the sharing of information as an industry with the government and among ourselves."

Sensors deliver that information. Bourge said sensors essentially record the state of OT networks, thereby observing any changes that occur, such as a new device added to the operating environment or communications with a new IP address. Any time such changes occur, the sensors send an alert. Sensors can monitor the traffic itself – who and what is coming in and out of the system – to identify when suspicious behavior or communications are occurring or when vulnerabilities or threat actors are involved. Sensor technologies can help the utility be more aware of what is happening on its system and allow for a broader awareness and spotting of cyber tactics, techniques, and procedures (TTPs). More simply put, the sensors alert the utility when patterns and pathways that are known to be used by bad actors are touching your system. They also help identify new ones.

Problem: Resources; Solution: Collaboration

Here's one problem: Most utilities have not deployed enough OT sensors. "The big gap in cybersecurity is visibility into the operational technology systems we have," said Carter Manucy, director of IT/OT cybersecurity at Florida Municipal Power Agency. "Traditionally, when we installed many of our older systems, all we did was install them to do one special function, so we only watch for that one function. We're not watching the network for anything outside normal behavior. That's what these monitoring systems do: Catch the abnormal activity."

But most smaller utilities cannot afford these much-needed sensors.

Some systems could cost hundreds of thousands of dollars, even for small- to medium-sized utilities, Bourge said. Increasing scope and complexity could reach more than $1 million for deployment.

Condello and his team have been working on ways to get sensors deployed through a cooperative agreement with the U.S. Department of Energy's Office of Cybersecurity, Energy Security and Emergency Response (CESER). This effort is funded by a grant CESER awarded to APPA in 2020," said Amy Thomas, APPA senior director of government relations.

Condello, who runs a group funded by this grant, said deployment of OT cybersecurity technologies is only part of the solutions DOE hopes will result from its grant investment. The second goal is collective defense, where utilities take data they get from their sensor technology and share it with government entities and information analysis centers, which, in turn, makes information available to other utilities. The final goal is for utilities to integrate timely and actionable information into their systems to protect their critical assets. Toward that end, Condello and his team created the Cyber Defense Community, a group of 39 member utilities.

"We're providing a forum for collaboration and corroboration," said Condello. "With the community, we share information across our membership as to what challenges they've faced and what has worked in addressing them. We help utilities make informed decisions."

This includes good purchasing decisions on those much-needed sensors. Brian Chandler is general manager of Troy Utilities in Alabama, and a member of Condello's group. "We issued a very extensive request for proposals with a very long list of qualifications and specifications," Chandler said. "For a medium or small municipal utility to have done something like that on their own would have been extremely difficult."

Chandler's utility serves about 20,000 customers with 10,000 meters. He was working with people like Florida Municipal Power's Manucy and Branndon Kelley, senior vice president of technology at American Municipal Power, a joint action agency serving 134 member utilities in 10 states. Both Kelley and Manucy are members of the Cyber Defense Community.

The community evaluated all of the proposals that responded to an RFP, and 11 members of the community are working toward piloting the rapid deployment of sensors as part of the DOE grant money to support deployment. Troy, FMPA and AMP are among 11 utilities that will deploy these systems.

"Part of the requirement of this project is that anonymized threat data is to be passed back to the Department of Energy so they can see what is going on with threats that affect the electric industry and pass that knowl-

Milsoft Enterprise Accounting and Utility Billing

A 360-degree view of your consumers and the complete history of their relationship with your utility equips you to meet and exceed the needs of today's consumer and provide the ultimate consumer experience.

You shouldn't have to guess or wonder how things are going at any given moment. Through real-time reporting and analytics our system provides you with the information you need to know about your staff, your consumers, and your revenues.

Your customers expect more, and they get more with Milsoft
Find out more: www.milsoft.com • 800-344-5647

MILSOFT®
Utility Solutions

Providing Powerful Software for Power Systems Professionals Since 1989.
Enterprise Accounting & Billing • Financial Management • Work Management • Automated Customer Services
Engineering Analysis • Outage Management • GIS & Field Engineering • Communications

edge along," Chandler said. "The sharing of threats and incidents delivers huge benefits. It tells you what to look for, what to prepare for and what available fixes, if any, are out there."

Time to Act

While large joint action agencies like FMPA and AMP have staff to review threat data and take action, smaller utilities generally do not have those resources. This is why Kelley thinks joint action should eventually offer cybersecurity services.

"A sensor by itself is not going to do anything for you. It collects data, but it's not going to be able to take evasive action to prevent trouble or address threats," he said. "Sending anonymized data to a government agency is a good first step. It gives them information to identify patterns and threats out there. But if there's an actual threat happening in your system, you need to respond in real time. You may not have time to wait a couple days for instructions to come back to you."

What is more, cyber expertise extends beyond knowing what to do. It also encompasses knowing how to do it and having both the time and skill to remediate the threat quickly, Kelley said. He advocates for cybersecurity managed services delivered by what he calls "super joint action agencies," such as Hometown Connections, which can aggregate requirements and deliver programs and services across the whole of public power regardless of how small or large they may be.

Florida Municipal Power Agency and several of its member utilities are working toward participating in the Cybersecurity Risk Information Sharing Program (CRISP), run by the Pacific Northwest National Laboratory and the Electric Information Sharing Analysis Center (E-ISAC). The program involves monitoring internet connections by installation of sensors and a server to support the CRISP application, which can cost more than most utilities' IT budget.

"Since a lot of the smaller utilities we support don't have enough data to tax that big piece of equipment, the concept is to put a smaller device at each utility and bring all that data back to the server in a secure manner," said FMPA's Manucy said.

The fix allows him to analyze data on multiple utilities simultaneously. It also keeps costs down because a smaller utility can participate for a few thousand dollars instead of a much larger installation cost, Manucy said. "This allows a smaller utility to participate without a huge capital outlay and large, ongoing maintenance costs."

Infrastructure Law Provides New Funding

The Infrastructure and Investment Jobs Act, signed into law in November 2021, will make money available to public power utilities hoping to strengthen their cybersecurity. One provision in the law directs the secretary of energy to provide grants and technical assistance for utilities to detect, respond to and recover from cybersecurity threats. The law appropriates $250 million to be distributed to municipal and cooperative utilities between 2022 and 2026.

Kelley thinks the potential for mandatory reporting of cybersecurity incidents will be one more reason managed services should be used to deal with threats. "Municipal utility workers are some of the most dedicated and smartest people ever. These people literally are doing seven jobs, which is why [public power] has the Seven Hats Award," he said. "Now cybersecurity is the eighth job. When this additional burden of mandatory incident reporting happens, it's something that should be managed or at least assisted with at the joint action level to alleviate that burden."

Mandatory incident reporting could be burdensome, but grid cybersecurity will be achieved only if everyone – utilities, government and industry groups – works together, said Manucy. "It's possible that sensor-based technologies could take the place of reporting requirements, but it's much too soon to know," he said. "However, by deploying sensors you gain the visibility required that you will need in order to comply, at some level, with these additional forthcoming laws."

To that end, Condello and his group are tapping members of the Cyber Defense Community for activities beyond funding of the cooperative agreement. "We recognize the community can contribute beyond this narrow investigation of OT technology for rapid deployment," Condello said. APPA is developing a cybersecurity guide for small utilities and has a risk-management working group. Community members will also help APPA plan a table-top security exercise that will be conducted at the Business & Financial Conference in September.

"The community is a gateway to knowledge-sharing and support to inform good decision-making," Condello said.