The Battle for Cybersecurity

From the national level to the local, the energy sector strives to protect members

By Brandon Pomrenke

Like any activity, crime evolves with time. Today's wide use of the Internet has given rise to cybercrime, which requires no physical proximity.

Today's cybercriminals are not the stereotypical band of hackers sitting in a dark room with computers and monitors casting an eerie glow. They work from just about anywhere with an Internet or phone connection. There is no need for supercomputers or physical access.

Because this threat is so commonplace, many in the energy industry work tirelessly to combat computer-related crime.

The energy industry may have a special draw to cybercriminals because of the importance of electricity to everyday life and because most Americans' information is stored somewhere in a utility's system.

A successful and broad-scale attack could set back parts of a local economy, its infrastructure and its ability to function reliably.

Those who work in the energy industry are aware of the risks to not only a reliable power supply, but to members' personal information—the prime target and moneymaker of cybercrime.

The Big Picture

National Rural Electric Cooperative Association Cybersecurity Lobbyist Bridgette Bourge believes cybersecurity is a priority for every level and type of energy provider, whether they are co-ops, munis, IOUs or government agencies.

Bourge explains, "Everyone is getting together and trying to find out, 'Where are the gaps, vulnerabilities and opportunities where we can help each other?'"

Bourge, whose computer network experience dates back to the Y2K days on Capitol Hill, believes working with and educating utilities and consumers can make a difference in today's technology-based world.

But information sharing may be one of the biggest challenges to keeping the energy sector secure against cybercrime, she adds.

"Information sharing among the industry, and from government to industry, is a major obstacle we're facing today to get a common operating picture and know where the largest cyber threats are," she said.

Photo by solarseven

To push through the information-sharing challenge, Bourge and others in the energy industry's corner have put together the Cybersecurity Information Sharing Act of 2015. The bill provides liability and Freedom of Information Act protection for utilities that report violations/attacks against their systems.

For smaller utilities that may lack the funding or staff size to support such a demanding task, this bill encourages information sharing with the government and agencies such as NRECA and the Electricity Sector Information Sharing and Analysis Center. The goal is gaining a better operational understanding of cyberattacks against the energy industry and working to combat them.

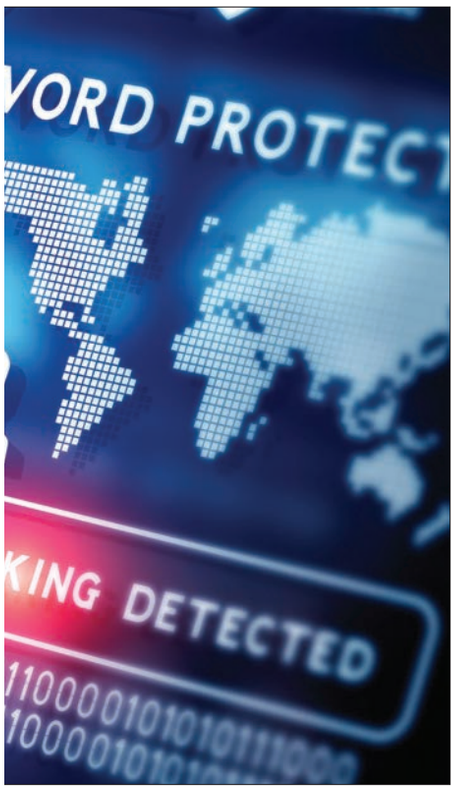
"Getting this bill through will allow a better common-threat operating picture for small, medium and large energy providers," said Bourge.

An example of this partnership's effectiveness comes from Consumers Power Inc., which covers approximately 3,500 square miles near Philomath, Oregon.

Within those 3,500 square miles are 22,000 meters. It takes quite a bit of effort—both on the ground and through the CPI network—to provide safe, reliable electricity to so much territory.

That is where information-sharing partnerships comes into play.

"There are services we can



partner with to share information," said CPI CEO Roman Gillen. "There are quasi-governmental service providers with access to federal information who are aware of hacking trends, worldwide and certainly in the U.S. They can combine that knowledge with security log information that we voluntarily provide them. In return, they keep us posted as to particular attacks that are trending in our area or our industry."

This relationship keeps national cybersecurity records up to date, and updates any local utility that could be directly affected.

"Security is a very complex and deep subject," said Gillen.

He hired a certified security firm to test the company's cybersecurity readiness.

"I immediately saw the value of having somebody with a critical eye look at our systems," Gillen said.

Bourge sees the willingness to work with outside agencies as one benefit of the energy industry's desire to protect member information and keep the grid safe.

"The electricity sector is the only sector that is regularly held up as an example for a public-private partnership in coordination," said Bourge.

She points out this sector is the only one with mandatory cybersecurity standards.

The standards give co-ops a set of guidelines to follow as a first line of defense against cyberattacks. In keeping with the tradition of information sharing and cooperatively creating guidelines, NRECA also has worked to create a template that cooperatives can use to formulate their own cybersecurity programs.

NRECA's Business and Technology Strategies team lead Maurice Martin sees these templates and guides as a solid first step in building a security program at utilities because they aid in risk management and cybersecurity planning.

He noted that current strategies may change throughout time.

"One project is researching next-generation monitoring to offer a more advanced approach to network monitoring to all co-ops," Martin said. "The project is gathering threat data from 10 co-ops around the country."

Those who work in the energy industry know the technical environment is constantly evolving. However, with dedication and know-how, it is possible to mitigate cyber risks.

"We'll never reach a point where we lean back in our chairs and wipe our hands on our laps and say, 'We've done it; we've arrived,'" said Gillen. "Our networks change over time. There are new devices and ways of doing things, new configurations and new equipment. The network changes regularly and new vulnerabilities are discovered. It's a continuing process of assessing where we are, checking fixes we think we've put in place and taking additional steps to make it more secure."

Gary Dodd, Bonneville Power Administration chief information security officer, also believes in taking all measures possible to protect infrastructure and information.

"I have intelligence analysts working 24 hours a day, seven days a week doing this work," Dodd said. "We have some people right now, and every minute of the day, hunting for persistent threats in the network."

The Human Factor

It is difficult to secure people and their practices, said Gillen.

"Particularly in the co-op world, we are friendly and trusting and cooperative," he said. "That's something that can easily be taken advantage of by people on the outside."

There are a variety of ways consumers can mitigate risks. Some are technical, others a little more practical.

For example, consumers should be careful when opening emails or clicking links embedded on unfamiliar websites. They should not provide credit card, banking or other personally identifiable information by phone.

Understanding information security is important not just for those who have information in the system, but also for those who have access.

BPA tests its employees by sending internal test emails with false links, explained Dodd.

"If employees click on the bad link I've sent them, it takes them to training that shows them how to recognize those," he said.

Cybercriminals can be convincing. It is their job to get your information.

"Cybercriminals are after any information they can sell," said Bourge.

Dodd agrees. When comparing whether hackers prefer affecting the grid or getting their hands on personally identifiable information, he thinks the latter is preferred.

"I think it's a combination of the two," said Dodd. "But personally identifiable information wins hands-down because there is a financial reward."

Regardless of why the threat exists, those working in the energy sector focus on how they can protect member information and what precautions they must take.

"Cybersecurity is no longer just an interesting conversation," Dodd said. "It's an absolute must." ■