Public Power Daily
A daily news service of the American Public Power Association

Thursday, October 24, 2013

Cyber and physical security plan is key to risk management, Crisson says

SEATTLE—A plan for cyber and physical security is a key element of a utility's risk management strategy, APPA President and CEO Mark Crisson told a gathering of utility lawyers here Oct. 22. The need for cybersecurity, in particular, is a fairly recent development that has presented itself in the last five or six years, he said. He spoke at APPA's Legal Seminar.

"We felt like we had a good handle on the issues, but it's rapidly evolving," Crisson said. Utilities cannot be complacent, because the threats are changing all of the time, he said.

In "the era that was, you'd hear about a lone hacker, or a disgruntled employee," or an industrial spy, he said. "Today, we've got some new threats that are more insidious."

There are botnets, where hackers take over a group of computers. "Hacktivist" groups—a dispersed group of hackers working together—are another, he said. Nation-states are involved as well. Earlier this year, China appeared to be behind some hacking efforts, he noted.

Mandiant, an American computer security company based in Alexandria, Va., released a 60-page study in February concluding that China's government is likely behind a series of cyber attacks on dozens of U.S. corporations and government agencies over the past several years. (See *Public Power Daily*, Feb. 20, 2013.)

"There are teams of cyber warriors," Crisson said. "These threats are evolving every day."

In Iran, the Stuxnet worm got into centrifuges and caused them to self-destruct. In Saudi Arabia, the Shamoon virus destroyed thousands of computers at the oil company Aramco, he said. Denial-of-service attacks have hit financial institutions, and also a public power utility: JEA in Jacksonville, Fla., had one that did not destroy equipment, but forced computers to shut down.

"There are physical threats, too," Crisson said. Five people with high-powered rifles shot up Pacific Gas & Electric Co.'s Metcalf substation. "If they had wanted to, they could have permanently disabled the substation," he said.

The "defense-in-depth" model used by the military can be helpful for utilities as they try to protect themselves against cyber and physical threats, Crisson said. You define your assets, define the threats, and then place your highest priority assets in the innermost level of protection. This way, if an attack comes, the first layers to be hit will be the less critical ones.

It is a good idea to look at a utility's operations—including SCADA, distribution automation and advanced metering—and examine whether these operations share any systems with the utility's enterprise departments or information technology departments, such as accounting, human resources or the utility's website, he said. "Make sure that one doesn't provide a back door to the other."

An executive order and presidential policy directive issued by President Obama in February 2013 calls for the identification of critical infrastructures whose loss would have "catastrophic regional or national effects." The executive order calls for information-sharing and collaboration with owners of critical infrastructure in 16 sectors, including energy. Of the 16 sectors, "we are the only one subject to mandatory requirements," Crisson said.

It makes sense to share information, he said. This can be difficult, however, when dealing with the federal government, he said. Officials talk about how dire the threats are, "but when we ask for more information, they say, 'You can't have it, because it's classified.'"

The National Infrastructure Advisory Council includes representatives from the 16 "critical infrastructure" sectors recognized by the federal government. In 2010, this group recommended increased dialogue between the electricity sector and government at the highest levels, Crisson said.

APPA, together with the Edison Electric Institute, Nuclear Energy Institute and National Rural Electric Cooperative Association, requested this type of dialogue, and the government responded and engaged in that beginning in 2012, he said.

Thanks to this collaboration, a new, revamped Electricity Subsector Coordinating Council had its first meeting with the Energy Department, Department of Homeland Security and the White House on Sept. 27, he said. Crisson, as well as the CEOs of EEI, NEI and NRECA, are on the ESCC's nine-member steering committee.

"We're already seeing progress" in information- and technology-sharing, Crisson said.

One of the results of the Sept. 27 meeting is "a recognition that we may need to learn more about EMP [electromagnetic pulse] and geomagnetic disturbances," he said. It's difficult to know what can be done about these, though, he said: "A solar flare is not something you can control."

Crisson encouraged attendees of the Legal Seminar to sign up to get cybersecurity information from the Electricity Subsector Information Sharing and Analysis Center, known as ES-ISAC. This center is operated by the North American Electric Reliability Corp. and all electric utilities are eligible to be members.

ES-ISAC provides advisories and alerts on real-time threats, vulnerabilities and plans for the electricity sector. It is set up to be separate from other programs run by NERC, including NERC's reliability standards and enforcement operations.

In June, APPA created a group made up of 20 of the association's member utilities, plus APPA staff. The committee, called the Cyber and Physical Preparedness Committee, meets regularly. It was formed in response to a collective recognition that "a more concerned effort needs to be placed on protecting our infrastructure from attacks, whether cyber or physical in nature," Crisson said earlier this fall. (See *Public Power Daily*, Oct. 1). — JEANNINE ANDERSON