NARUC Release of Cybersecurity Guidelines Should Have Utility Companies on High Alert

02.07.2017 | By Jill N. Jaffe

On January 30, 2017, the National Association of Regulatory Utility Commissioners (NARUC) released Version 3.0 of Cybersecurity A Primer for State Utility Regulators. This cybersecurity overview is an important reminder to public utilities to be prepared for cyber threats.

Then again, public utilities probably don't need a reminder after a cybersecurity event that occurred at the end of last year. In December 2016, the Burlington Electric Department reported the presence of malware on one of its employee's computers. The computer was not connected to the electric grid at the time, and the utility quickly isolated the laptop and coordinated with federal authorities to eradicate the problem. But, it was still a nerve-wracking development – experts have long warned that public utilities could be targeted because of the wide-spread impact a well-executed hack could have. And here, even though the electric grid was not compromised, it still became a public relations headache because several news outlets incorrectly reported that the malware-infected computer was, in fact, connected to the grid, endangering vital infrastructure.

In light of increasing threats, state and federal regulators are developing guidance documents, and several state public utility regulators have prepared cybersecurity action plans, such as Connecticut. The American Water Works Association (AWWA) also recently released guidance for water utilities regarding the protection of systems infrastructure. This momentum is likely to lead to increasingly stringent regulatory requirements regarding cybersecurity plans, policies, and practices for public utilities in the United States.

These guidance documents are also valuable tools for public utilities, particularly small and midsize utilities that are looking to strengthen their cybersecurity protections but may not have the resources to implement a plan from scratch. The leading thinkers in this area advocate that public utilities develop cybersecurity plans to protect three different operational components: information technologies systems, operations technology and controls systems (i.e., SCADA systems), and the smart grid. While protecting IT systems falls

within the gambit of traditional cybersecurity planning, the latter two areas are more unique to the public utilities industries. A public utility's data security breach plan should address all three functional areas with respect to how it will defend its systems as well as how it will respond in the event of a potential breach.

Resources from institutions like NARUC or AWWA provide invaluable insights on how public utilities can take steps to protect the unique features of their operations. Unfortunately, cyber threats are not going away, so public utilities must be prepared.