Bond Case Briefs

Municipal Finance Law Since 1971

As Water Utilities Move Online, Hackers Take Note.

America's power grid has gotten a lot of attention, but water utilities are increasingly vulnerable to cyberattacks.

The Department of Homeland Security (DHS) released a report last year that showed the nation's water grid, not just its electric grid, was also vulnerable to attacks by hackers. In fact, water utilities were most likely to have reported what DHS categorizes as an advanced persistent threat, which involves exploiting flaws in software programs that run water valves and controls, among other things. The worst kind of these attacks can go undetected for long periods of time.

Water utilities have in recent years — like pretty much everything else — become more reliant on the Internet to operate its networks of pipes and pumps. These controls can help monitor conditions around the clock and the benefits for both water and electrical utilities can be greater reliability and lower labor costs as fewer workers are needed to monitor the valves, controls and switches.

But hackers are looking for ways to test the vulnerabilities of critical infrastructure, and while so much attention has been paid to America's power grid, water utilities are particularly exposed. Hackers and state-sponsored terrorists are "mapping the control systems for water and wastewater [systems] to understand where the controls systems are located," says Dr. Paul Stockton, a former assistant secretary of defense and managing director of Sonecon, a Washington-based security consulting firm. "This kind of mapping could be preparatory work in anticipation of attacks that are designed to disable and disrupt critical infrastructure."

Indeed, the FBI confirmed in 2014 that operatives in China, Iran and Russia were doing just such a mapping operation, looking for cybersecurity weaknesses in the country's water and electric infrastructure.

In case of such an event or a natural disaster, most utilities operate mechanical backup systems. But maintaining a dual control system is expensive. "Utility companies want to reduce their costs as they transition to a new generation of industrial control systems," says Stockton. The risk is that "they will stop maintaining these backup systems and stop retaining the staff that operate them."

To keep utilities running backup systems, Stockton and other experts suggest that public utility commissions and the feds help utilities recover the costs of running two systems while also investing in promising strategies to protect infrastructure from cyberattacks. State regulators could also help reduce risks by working more collaboratively with federal regulators to push utilities to focus on creating comprehensive cybersecurity strategies rather than just complying with regulatory requirements, according to a report by the Government Accountability Office.

Other methods for mitigating a possible cyberattack on water infrastructure include the adoption of a set of standards for the entire industry; better sharing of information by utilities about cybersecurity vulnerabilities, incidents and best practices; and stronger requirements that smart grid and water control systems have built-in security features.

If all else fails, the National Governors Association’s Council of Governors has developed plans for a cybersecurity National Guard that would provide a unified response in the event of an attack that disrupts, damages or destroys utilities. Let’s hope it’s not needed.

GOVERNING.COM

BY TOD NEWCOMBE | FEBRUARY 2016