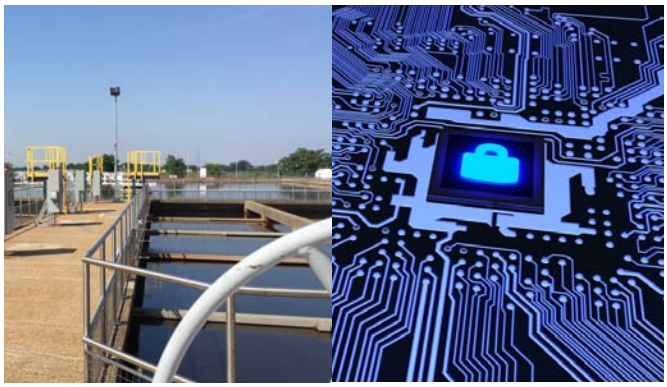
WATER QUALITY & HEALTH COUNCIL
PERSPECTIVES

Cyber Security 101 for Drinking Water

By Steve Hubbs, PE
October 5, 2018



As we move closer to another new decade in the not-so-new millennium, it seems a safe bet that virtually everyone reading this article is familiar with *cyber security*. By now, many readers have been personally affected by a breach in cyber security. Despite being celebrated as a U.S. public health triumph, drinking water utilities are not immune to cyberattacks, which according to one recent article, continue to grow.

Cyber Threats to Water Utilities

As a critical infrastructure sector, the U.S. drinking water community remains committed to providing safe, treated water to all of its customers. But many utilities, particularly small systems, may lack adequate resources to establish, let alone maintain, an up-to-date cyber security program. Further, a false sense of security may persist that cyberattacks do not present a risk to *their systems*. But the results of a recent cyber security audit of water, electric, and natural gas utilities by the State of Connecticut prove otherwise: "During the past year, both the volume and sophistication of [combined] attempts to penetrate and compromise Connecticut's public utilities increased…varying from a few thousand to over 10 million per week, coming from every continent." Fortunately, that state was able to repel myriad cyber threats from powerful e-viruses, malware, and other automated attack vectors.

According to the U.S. Environmental Protection Agency (EPA) Water Sector Cybersecurity Brief for States, cyberattacks on water utilities and automated controls systems like SCADA (systems control and data acquisition)[1] can cause service disruptions and real harm, including:[2]

- Upset treatment and conveyance processes by opening and closing valves, overriding alarms or disabling pumps or other equipment;
- Deface the utility's website or compromise the email system;
- Steal customers' personal data or credit card information from the utility's billing system; and
- Install malicious programs like ransomware, which can disable business enterprise or process control operations.

Cyber Security Breaches of Water Systems

[1] SCADA and other industrial control systems are standard in medium and larger drinking water utilities and are being increasingly used by smaller systems to manage water treatment processes like disinfectant addition.
[2] https://www.epa.gov/sites/production/files/2018-06/documents/cybersecurity_guide_for_states_final_0.pdf.

Cyber-aggressors like cyberthieves can compromise the ability of water utilities to provide clean and safe water, harm the environment, erode customer confidence, and result in financial and legal liabilities for the utility and, ultimately, customers. According to a recent American Water Works Association (AWWA) feature on cyber security, to date, the greatest motivation for cyberattacks in general has been financial—either directly through ransom requests or taking data to sell. In 2016, the Lansing (Michigan) Board of Water & Light (BWL) was breached and locked via ransomware by unidentified foreign hackers, which started simply with an employee opening an email attachment. According to a *Lansing State Journal* article:[3] "In addition to paying a $25,000 ransom to unidentified foreign hackers, BWL incurred costs of cyber forensics, the cleaning and testing of 700 to 800 laptops, desktops and servers, the replacement of an extensively infected server, and $400,000 in cybersecurity upgrades that brought the total to about $2.4 million."

On a smaller scale, hackers took control of the cellular routers and stole valuable internet service from one U.S. water utility from late 2016 to early 2017, raising the authority's cellular data bill from an average of $300 a month to $45,000 in December and $53,000 in January. Thankfully, in both preceding cases, those cyberthieves did not seek to disrupt water supply and treatment. An older, but notorious cyberattack against a wastewater treatment plant occurred in Queensland, Australia, in 2000, and resulted in raw sewage spilling into neighboring rivers, parks, and the grounds of a nearby hotel. The attack was conducted by an insider who originally installed the radio-controlled SCADA system. Other recent, successful cyberattacks in the water sector have been reported, but remain rare.

Staying Ahead of Cyber Threats and Cyberattacks

Given the increasingly interconnected nature of cyber- and physical security in U.S. infrastructure, cyber threats to the provision of safe drinking water will only grow in the years to come. As reported by AWWA, in 2015, the U.S. Department of Homeland Security (DHS) responded to 25 cyber security incidents in the water sector, which increased from 14 incidents from the previous year. In 2014, the National Institute of Standards and Technology (NIST) developed the Cyber Security Framework (CSF) to help support and mitigate cyber threats to critical infrastructure sectors. AWWA has developed guidance and a "use-case" tool to support the voluntary application of the NIST CSF. Also, DHS, through its Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), provides numerous resources and information alerts that can help water systems build a cyber security risk management program and, at a minimum, stay apprised of threats.

Even when best practices for cyber security are applied diligently, SCADA and other automated systems can still be vulnerable to determined attackers, as was evident with DHS' reporting on cyber-activity targeting critical infrastructure sectors, including water systems. To conclude, if this article has seemed a bit sensational or alarmist in nature, let me put things in perspective: the United States has some of the best produced and protected drinking water in the world. For example, chlorine disinfection has virtually eliminated once-common waterborne diseases like typhoid fever. This did not happen overnight, and to be sure, continued cooperation and vigilance is needed to keep our drinking water both *safe* and *secure*. The drinking water community takes these threats very seriously, and is continuously addressing security issues, including cyber threats.

Steve Hubbs retired from water treatment operations at the Louisville Water Company in 2004. He remains an active volunteer in the drinking water community today.

[3] https://www.lansingstatejournal.com/story/news/local/2016/11/25/bwl-prepared-ransomware-attack/94332454/.