ADDITIONAL TECHNOLOGY TO HELP THWART CYBERATTACKS

The future is connected, but it must also be secure — especially when it comes to public water.

By Cody P. Bann

Water infrastructure is critical to national security, economic stability, and public health and safety. While necessary for operations, the increasing automation of the water sector has opened it up to malicious cyber activity that could disrupt or manipulate services. In 2009, President Obama declared cybersecurity threats to be among "the most serious economic and national security challenges we face as a nation."[1] In January 2012, the U.S. Director of National Intelligence also noted that cyber threats pose a critical national and economic security concern in testimony given before the U.S. House of Representatives.[2]

Over the past two decades, federal investment in water systems has equaled only 4% of the amount that state and local governments invested, and most of the federal funding was in the form of low-interest loans, not grants. Fortunately, the White House has earmarked $2 billion from the bipartisan infrastructure bill that was signed into law last year to go toward strengthening U.S. infrastructure against cyberattacks. This couldn't come at a more critical time, as cities such as Los Angeles, San Francisco, Portland, OR, and Oldsmar, FL have experienced hacks and the ongoing threats that the volatile geopolitical climate poses.

Water And Wastewater Infrastructure Security

After the September 11 attacks in 2001, George W. Bush's administration directed efforts to secure critical infrastructure through programs such as the National Strategy to Secure Cyberspace, which addresses the vulnerabilities of supervisory control and data acquisition (SCADA) and industrial control systems (ICSs) — essential to effective water utility operations — and called on the private sector to work with the government to provide trusted control systems. The Presidential Policy Directive of 2013, under President Obama, echoed President Bush's Homeland Security Presidential Directive in affirming that water was among the 16 critical U.S. infrastructure sectors that must be protected.[3]

There are close to 200,000 drinking water systems in the U.S. that provide tap water to nearly 300 million people. This critical infrastructure spans tens of thousands of miles, involves many remote sites, and requires multiple networks with complex software and hardware needs. The sheer size and scope of these systems offer hackers many exploitable entry points. As utilities transition to the cloud, remote access, smart devices, and the Internet of Things, IT and OT are no longer separate. Over the past decade, the technology behind water infrastructures and utilities has become more interconnected with OT and IoT devices. The various connected devices such as controllers, sensors, and smart meters are being used by water utilities to remotely monitor and manage processes. In a recent West Monroe survey, 67% of utility leaders cited cybersecurity as their top concern of the converged IT and OT network.

A cyberattack causing an interruption to drinking water and wastewater services could erode public confidence, or worse, produce significant public health and economic consequences.

"The diverse nature of the water and wastewater sector, with organizations of varying size and ownership, the sector's splintered regulatory regime, and a lack of cybersecurity governance protocols, presents significant cybersecurity challenges, states a report by the American Water and Works Association (AWWA), *Cybersecurity Risk & Responsibility in the Water Sector*. "Moreover, entities within the sector often face insufficient financial, human, and technological resources. Many organizations have limited budgets, aging computer systems, and personnel who may lack the knowledge and experience for building robust cybersecurity defenses and responding effectively to cyberattacks."[4]

Remote Alarm Notification Software Offers Additional Security

The AWWA further warns: "Failing to address cybersecurity risk in a proactive way can have devastating results. Failing to take reasonable measures and employ best practices to prevent, detect, and swiftly respond to cyberattacks means that organizations and the people who run them will face greater damage — including technical, operational, financial, and reputational harm — when the cyberattacks do occur."

Utilities face myriad challenges to managing cyber risk due to varying water and wastewater infrastructure and entities of vastly different sizes, capabilities, resources, and types of ownership. However, turning to additional technology is one answer.

AWWA acknowledges — and many utilities have become aware — that replacing legacy systems and networks can be extremely costly. However, it is nonetheless essential to work with cybersecurity experts and solutions providers to update, if sufficient, or overhaul outdated systems. Experts can help to prioritize risk with a cybersecurity plan that, at minimum, complies with basic standards to restrict physical and technical access via firewalls, logging, and encryption, etc.[5]

Additionally, many SCADA systems are simply overexposed to the internet by remote desktop applications (e.g., Remote Desktop Protocol [RDP] and TeamViewer). In an attempt to provide process and asset information to operators, organizations have provided much more, ignoring the principle of least privilege and opening their entire control systems and their hosts to remote desktop access by hostile parties. Such broad remote access techniques present an increased security risk for organizations, a risk that Oldsmar experienced firsthand last year when an improperly secured TeamViewer application allowed an unauthorized party to increase the amount of sodium hydroxide being added to its water treatment process.

Advanced remote alarm notification software allows remote operators access to only the information they need from SCADA, but not access to the SCADA itself or its operating system's host. Such notification software is compatible with more secure, layered networks in which a series of firewalls provides added protection from attacks. This is done by deploying notification solutions alongside the SCADA system at the network's control level and using notification modalities that are not internet-facing or distributing internet-facing notification processes to higher levels. For example, internal email servers, SMS modems, and voice via Private Branch Exchange (PBX) devices allow communication with the outside world without internet exposure. Likewise, separating the processes that interface with SCADA from those that interface with external email servers, Voice over Internet Protocol (VoIP) solutions, and cloud apps allows internet-based notifications without compromising security.

Of course, there are valid use cases for desktop sharing software that do not violate Principle of Least Privilege (PoLP) and go well beyond operator access to process information. For such systems, it's critical that the remote desktop solutions be implemented with sound security.

There are several steps that utilities should take to improve their cybersecurity:

- Updating to the latest versions of software;
- Employing multifactor authentication;
- Using strong passwords to protect RDP credentials; and
- Ensuring that anti-virus systems, spam filters, and firewalls are secure, properly configured, and up to date.[6]

Utilities should also take steps to secure any remote access software. They should not use unattended access features, and IT leaders should configure the software such that the application and associated background services are stopped when not in use.[7] Integrating the remote alarm notification software through the SCADA system is critical to further reducing cyberattacks.

The New Normal

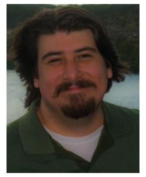
According to McKinsey & Company's report, *Critical resilience: Adapting infrastructure to repel cyber threats*, cyberattacks should be thought of as a certainty akin to the forces of nature. The report's authors advise: "Just as engineers must consider the heaviest rains that a dam may need to contain in the next century … those digitizing infrastructure must plan for the worst in considering how an attacker might abuse or exploit systems that enable infrastructure monitoring and control."[8]

It's a sobering, but essential, recommendation, for as important as connected infrastructure will be for the future of utility management, the safety of our water systems remains paramount. ■

References:

1. Robert M. Clark, Srinivas Panguluri, Trent D. Nelson, Richard P. Wyman, "Protecting Drinking Water Utilities From Cyber Threats," 2016.
2. Ibid
3. Ibid
4. https://www.awwa.org/Portals/0/AWWA/Government/AWWACybersecurityRiskandResponsibility.pdf (accessed March 1, 2022).
5. Ibid
6. https://biztechmagazine.com/article/2021/04/cybersecurity-lessons-utilities-can-learn-oldsmar-water-plant-hack (accessed March 1, 2022).
7. Ibid
8. https://www.mckinsey.com/industries/travel-logistics-and-infrastructure/our-insights/critical-resilience-adapting-infrastructure-to-repel-cyberthreats (accessed March 1, 2022)

About The Author



Cody Bann is director of engineering at Austin, TX-based WIN-911 and may be reached at cody.bann@win911.com. The company helps protect over 18,000 facilities in 85 countries by delivering critical machine alarms via smartphone or tablet app, voice (VoIP and analog), text, email, and in-plant announcer, reducing operator response times, system downtime, and maintenance costs. For more information, visit www.win911.com/.