1898 & CO.
PART OF BURNS McDONNELL

WHITE PAPER

Keeping Water Treatment Operations Safe from Cyberthreats

By Jason Vigh, 1898 & Co., and Jake White, PE, Burns & McDonnell

Every municipal utility has a primary objective: to deliver safe, reliable services to the community. Achieving this objective requires designers and operators of water and wastewater treatment facilities to address a broad range of microbial, physical and chemical risk factors. Cybersecurity threats to the operational technology (OT) landscape should now be part of this list.

In February 2021, hackers gained unauthorized remote access to a water treatment plant's computer system in Oldsmar, Florida, and attempted to increase the sodium hydroxide in the drinking water to potentially dangerous levels. This triggered a new wave of national concern throughout the water and wastewater industry. However, cyberthreats to drinking water systems are nothing new. In March 2019, the Ellsworth County Rural Water District in Kansas was hacked.

While these hacks were mitigated before the drinking water supplies were negatively impacted, these incidents immediately reminded utilities of their own potential cyber vulnerabilities — both known and unknown. As utilities now consider what to do about such vulnerabilities, many will discover a valuable lesson: Cybersecurity risks are similar to other risks that threaten the safety and reliability of water and wastewater treatment services. With appropriate mitigation strategies, such risks can be controlled, delivering benefits that far outweigh the cost of implementing a resilient operational technology (OT) cyber program.

Utilities already factor a wide range of risks and hazards into the design, construction, operation and maintenance of water and wastewater treatment facilities. Now, cybersecurity safeguards should be integrated into these processes as well, with the goal of building greater resiliency into water supplies.

A Common Dialogue

Suppose a city is interested in doing a plant upgrade, including new programmable logic controllers (PLCs), instrumentation and remote access and monitoring capabilities. The city's project manager would commonly engage an engineering firm to consider all the risks associated with such a project. Cybersecurity would likely

arise in conversations about defense strategies such as firewalls. However, recent events suggest that traditional defense strategies are no longer be robust enough to protect against hackers.

A utility's success in managing cybersecurity risks is measured by its ability to detect, respond to and recover from cyber intrusions and other nefarious cyber activity. To bolster resilience, facilities require effective mitigation strategies, along with detection and response capabilities that operate around the clock to protect critical systems. All are necessary for new greenfield projects as well as existing facilities, regardless of size or age.

The process for creating more resilient water and wastewater systems involves three basic steps:

1. **Create a cyber risk profile**. While creating a risk profile is a common process for operators, cybersecurity presents a new risk frontier. Before implementing new cybersecurity measures it is important to understand the utility's current cybersecurity capabilities. This requires taking a close look at the policies, procedures, people and technologies already in place at treatment plants and other infrastructure.

   For existing plants, this profile should be incorporated into a utility master plan or other planning documents for any rehabilitation projects. The profile is necessary when assessing current operations for adherence to the current cybersecurity status. The assessment would carefully look at supervisory control and data acquisition (SCADA) systems, industrial control systems (ICS) and safety instrumentation systems that may currently be short on protections.

   Treatment processes and other automated or digitized systems should therefore be evaluated to assess vulnerabilities and identify any existing gaps. Similarly, greenfield projects that undergo this assessment during the planning process can produce a cyber risk profile that guides designers to integrate cybersecurity solutions into facility and system design from day one.

2. **Close any cyber gaps**. A cyber risk profile details the specific known cybersecurity risks a utility faces. This information will prove invaluable when making decisions on solutions to harden systems against cyberattacks.

   The cracks in current systems, albeit small, can represent access points to parties seeking to cause disruption in systems. In the Oldsmar, Florida, attack, hackers targeted the chemical systems that control water quality and safety. Other attacks could be designed to target electrical systems with the goal of causing power outages or equipment malfunction. Still others could seek opportunities to manipulate sensor readings and force user errors.

   Once identified, high priority gaps should be addressed first with basic risk mitigation strategies. Breaches in control systems must be patched and open ports should be closed. In some cases, software factory settings must be modified with strict set points to protect against cyber manipulation.

   Basic cyber hygiene practices such as anti-malware, hardening, patch management and antivirus programs are great defenses that can deter intrusion. Unfortunately, these solutions alone are insufficient. An enhanced zero-trust security approach, which leverages strong segmentation and adds user and device authentication, now ranks among the top defense and preventive cybersecurity strategies.

   Characterizing and tracking cyber risks is made easier when integrated into a utility's risk model, frequently created to address a range of possible equipment and system failures. If models do not already include a failure mode for cyber incidents, utilities should consider adding one. Failure information in a risk model not only helps inform the response to an incident, but it can also point designers to cybersecurity risk mitigation strategies to prevent future failure.

3. **Monitor continuously**. Closing security gaps and hardening facilities are the first steps of the cybersecurity mitigation process. Resilient water or wastewater systems require continuous monitoring to detect if and when hackers may try to penetrate operations. Should a breach occur, utilities need mechanisms that speed up the response to, and recovery from, the attack.

   These monitoring systems should be automated for several reasons. First, an OT cyber incident should not be left to the detection of a staff member because human monitoring requires a significant number of employee resources. Utility staff time is better spent focusing on the core business of operating the site, rather than on 24/7 lookout for potential system breaches. Cybersecurity detection also requires specialized knowledge and immediate responses that can often be above and beyond the training, experience and reflexes of operational staff. For unattended facilities in particular, automated eyes and ears are the only option.

The trends and risk factors that drive cyberthreats also evolve over time, sometimes with national security implications. More frequent and effective monitoring makes it possible to address changing demands and speed communication to staff and leadership who need it.

Protecting the Water Supply and Utility Reputation

Protecting against every cyberthreat a plant may encounter may seem like a steep hill for a water and wastewater utility to climb, but it doesn't need to be. Designing or rehabilitating operations with cybersecurity in mind will go a long way toward delivering a safe and reliable water supply.

While fending off a wide range of potential intrusions, cybersecurity solutions can also help utilities achieve goals for effective and secure connectivity, process optimization and system integration. Utility customers will likely welcome news of these protections as well.

Cybersecurity risks should now be discussed and mitigated like any other risk that threatens a utility's ability to fulfill its mission. These risks should be addressed in and integrated into the design, construction, operation and maintenance of facilities.

About 1898 & Co.

1898 & Co. is a business, technology and cybersecurity consulting firm serving the industries that keep our world in motion. As part of Burns & McDonnell, our consultants leverage global experience in critical infrastructure assets to innovate practical solutions grounded in your operational realities. For more information, visit **1898andCo.com**.

About Burns & McDonnell

Burns & McDonnell is a family of companies bringing together an unmatched team of engineers, construction and craft professionals, architects, and more to design and build our critical infrastructure. With an integrated construction and design mindset, we offer full-service capabilities. Founded in 1898 and working from dozens of offices globally, Burns & McDonnell is 100% employee-owned. For more information, visit **burnsmcd.com**.

1078108-0824