POINT OF VIEW

Protecting Water and Wastewater Systems

Strategies for Securing Critical Infrastructure

Executive Summary

Clean water is essential to life, and the safe operation of water and wastewater services is considered a fundamental critical infrastructure sector. The industry faces increasingly broad and serious cyberthreats from criminals intent on extorting money and nation-states aiming to disrupt essential services for political or military ends. Many utilities lack basic cybersecurity tools and practices, such as staying current on software updates, making them vulnerable to even relatively unsophisticated threats. To better protect their systems and improve cyber resilience, organizations must implement basic cybersecurity measures and best practices across both information technology (IT) and operational technology (OT) networks.

In a 2024 survey of municipally owned and operated systems, 33% of respondents reported at least one attack in the last 12 months.[1]

The Impact of Cyberattacks on Water Systems

Communities depend on water systems and treatment plants, but these facilities are increasingly vulnerable. Critical infrastructure, such as water and wastewater systems, often lacks adequate cybersecurity measures, particularly at smaller utilities and service providers. Some lack cybersecurity expertise and, in many cases, even basic cybersecurity tools, so water and wastewater utilities are often a soft target for criminals and nation-state actors. Attacks may involve tampering with controls, interfering with chemical treatments, disrupting water flows, or encrypting systems and holding them for ransom. Water utilities are beginning to use technologies such as unmanned aerial vehicles (drones) to improve their operational efficiency but this technology has also been used by malicious actors to mount physical or cyberattacks on service providers.[2]

As the prevalence, speed, and impacts of cyberattacks continue to increase, water-related utilities and agencies need to invest more time, money, and effort in cybersecurity. However, they often face human and financial resource challenges. In some cases, small utilities that have historically paid little attention to cybersecurity don't even know where to start.

Cybersecurity Guidance for Water and Wastewater Organizations

In May 2025, the American Water Works Association (AWWA) released a revised version of its Water Sector Cybersecurity Risk Management Guidance, a comprehensive resource designed to help organizations in the water sector better manage cybersecurity risks.

Getting started

The AWWA guidance outlines an approach based on a three-phase maturity model for incrementally improving cybersecurity in water systems. Phase 1 focuses on establishing cybersecurity fundamentals. Phase 2 involves conducting a cybersecurity assessment and developing a cybersecurity risk management plan specific to each organization, and Phase 3 is the implementation and continuous refinement of the plan.

The guidance is comprehensive and applicable for utilities ranging from big city utilities with dedicated cybersecurity staff to small rural providers who lack both expertise and funding. While at virtually every utility, someone is responsible for cybersecurity, especially in smaller utilities, this may be one of many functions they perform. But taking a few basic steps can make a huge difference in overall cyber resilience.

In March 2024, the Environmental Protection Agency sent a letter to governors emphasizing the need to safeguard the U.S. water and wastewater systems against cyberthreats.[3]

AWWA foundational practices

For organizations just starting to focus on cybersecurity, a good place to begin is by creating a cyber risk management program and implementing a few foundational practices. Appendix B of the AWWA guidance provides a detailed roadmap; however, effective cybersecurity in the IT and OT systems of water and wastewater utilities typically begins with the following activities.

Process improvements

- **Create a cyber-incident response plan.** This plan should be developed and regularly exercised.
- **Set up software and program backups.** Regular backups of critical data and software must be maintained and tested for recoverability.

People and culture

- **Ensure leadership commitment.** To foster a culture of security, leadership commitment is essential.
- **Allocate resources for cybersecurity improvements.** There should be a dedicated budget line item for cybersecurity improvements, along with a multi-year plan for implementing enhancements. Budget allocations should also be adjusted based on periodic risk assessments.
- **Appoint leadership.** A defined cybersecurity risk management leader should be appointed, and the person's responsibilities should be clearly outlined.
- **Conduct training and education programs to promote cybersecurity awareness.** All system employees should receive periodic cybersecurity training that covers topics such as phishing, password security, and incident reporting.

Technology

- **Remove non-essential OT devices from the public internet.** Create a list of all internet-connected devices and public IP addresses assigned to the system and remove Internet access to any devices that don't absolutely require it. All essential internet-connected devices should be behind a firewall.
- **Secure remote access.** The system should have an Industrial Demilitarized Zone for secure remote access, and multi-factor authentication should be required for all remote access solutions. Unique usernames and passwords must be assigned to each user, with no shared accounts.
- **Set up usernames and passwords.** Each user must have a unique username and password. Password management best practices should be enforced, and generic user accounts should be prohibited. Implement a central authentication service, such as Microsoft Active Directory, for password management.
- **Manage default passwords.** Default passwords on all devices must be changed to mitigate vulnerabilities.
- **Implement network monitoring.** Network traffic should be monitored for malicious activity to detect cyber incidents.

How Fortinet Can Help

Fortinet offers cybersecurity solutions for water and wastewater utilities to protect both their IT and OT networks. Fortinet solutions can secure remote infrastructure, such as river intakes and boreholes, as well as internal treatment processes and pumping stations, from cyberattacks that could disrupt the water supply and affect public health.

By deploying Fortinet security products, including firewalls, switches, and agents, water utilities can gain enhanced network visibility, streamline management, and improve performance while safeguarding sensitive data and critical infrastructure from cyber threats. Discover how Fortinet helps public utilities secure their systems and our industry-leading OT Security Platform, which features ruggedized hardware for deployment in even the harshest environments.

[1] Wastewater Digest, Fortinet 2024 Water Utility Cybersecurity Report, 2024, https://www.fortinet.com/content/dam/maindam/PUBLIC/02_MARKETING/08_Report/2024-Cybersecurity-in-Water-Management-Facilities-Report.pdf.

[2] Industrial Cyber, EPA, WaterISAC caution utilities on drone threats and cyber risks in evolving security landscape, August 18, 2025, https://industrialcyber.co/utilities-energy-power-water-waste/epa-waterisac-caution-utilities-on-drone-threats-and-cyber-risks-in-evolving-cybersecurity-landscape/.

[3] U.S. Environmental Protection Agency, Letter to Governors, March 18, 2024, https://www.epa.gov/system/files/documents/2024-03/epa-apnsa-letter-to-governors_03182024.pdf.

September 22, 2025 11:39 AM / MKTG-2069-0-0-EN