WFX
WATER FINANCE EXCHANGE
NO COMMUNITY LEFT BEHIND

COMMUNITY RESOURCES

Cybersecurity - Best Practices for Water Systems

What is Cybersecurity?

Cybersecurity is the practice of protecting systems, networks, and programs from digital attacks that can prevent a system from functioning correctly. Cybercriminals can infiltrate digital systems, programs, and networks through methods like hacking, email phishing, ransomware attacks, and data theft. Cybercriminals have also been able to steal customer's personal data, including billing information such as banking or credit card data.

Why is Cybersecurity Important?

Cybersecurity is a critical element of safe and effective water system management, as well as capacity-building by digitizing and protecting important information. Cybercrimes can place water systems, their employees, and their customers in danger of financial theft, information theft or public health crises.

Small Community Water Systems Are at Risk for Cybersecurity Breaches

Water systems are a vital component of public health and safety, which makes them a target for cybercrime. Cybercriminals can access water system and other networks remotely with only a computer and an internet connection. This allows them to access account information and manipulate automated or digitized processes. causing interruptions in treatment, pumping and distribution. In light of increasing cybersecurity threats, new laws have been passed that require water systems serving more than 3,300 customers to implement cybersecurity measures.

The American Water Works Association (AWWA) notes that small, rural water systems, who often operate with fewer resources, may struggle with establishing cybersecurity standards, as the process can be time consuming, while threats and attacks continue to increase.

What steps can my water system take to improve its Cybersecurity?

Water systems can take action to reduce the risk of a cybersecurity attack by:

- Becoming familiar with existing cybersecurity laws, guidelines, and resources
- Assigning a point person for cybersecurity
- Pulling together a task force to implement and maintain cybersecurity procedures
- Reviewing and leveraging the cybersecurity resources from CISA, AWWA, and WaterISAC
- Developing and implementing a plan for cybersecurity standards
- Regular monitoring of cybersecurity standards and potential threats
- Conducting regular trainings or drills to ensure staff are prepared for potential events

What resources are available to help improve Cybersecurity?

Government entities like the National Institute of Standards of Technology (NIST) at the Department of Commerce and the Cybersecurity & Infrastructure Security Agency (CISA) have published a range of options to reduce the risk of a cybersecurity breach for water and wastewater systems.

COMMUNITY RESOURCES - CYBERSECURITY

NIST's Five Key Ways to Reduce Risk

1) Designate people responsible for carrying out cybersecurity policies

2) Protect data (engineering, financial, business ops and customer data)

   a. Implement cybersecurity trainings. If feasible, implement private VPNs.

3) Detect

   a. Train staff how to identify cybersecurity breaches

   b. Establish a reporting process and procedure for staff if they think there's been a breach (lost equipment, unauthorized users in the system, confidential data sent to the wrong person)

   c. CISA and WaterISAC both have reporting features on their websites

4) Respond - Establish and practice procedures in the event of a confirmed or suspected cyber-attack (reporting the incident to the cybersecurity lead, reporting the incident to CISA, changing passwords)

5) Recover

   a. Responses should include methods to recover lost property or restore breached databases (reporting the incident to local law enforcement, working with a third-party cybersecurity team)

   b. In some cases, lost information may not be recoverable. In these situations, some equipment may need to have their information and data deleted or replaced, or security passwords will need to be changed.

CISA's Top Actions for Securing Water Systems

- Reduce exposure to public-facing internet (any internet applications accessible to the general public)
- Conduct regular cybersecurity assessments such as EPA's free Water Cybersecurity Assessment Tool.
- Change default passwords immediately
- Conduct an inventory of operational technology/information technology assets
- Develop and exercise cybersecurity incident response and recovery plans. CISA has an incident response guide available in English and Spanish.
- Back up, or create a copy of, operational technology (OT)/information technology (IT) systems
- Reduce exposure to cybersecurity vulnerabilities, which are weaknesses within a software, computer system, or network that make an entity more susceptible to cybercrimes. Specific vulnerabilities can be researched on CISA's Known Exploited Vulnerabilities (KEV) Catalog.
- Conduct cybersecurity awareness trainings for all staff. Organizations like AWWA and the Environmental Protection Agency (EPA) offer trainings.

There are also many tools for reducing risks specifically for water systems, including:

- CISA's free water system cyber vulnerability scanning
- CISA's free cyber hygiene services
- American Water Works Association (AWWA)'s assessment tool and guide

COMMUNITY RESOURCES - CYBERSECURITY

How Cybersecurity Requirements are Changing in the Water Sector

America's Water Infrastructure Act (AWIA) Section 2013 of America's Water Infrastructure Act of 2018 requires Community Water Systems (CWS) serving more than 3,300 people to prepare and/or revise risk and resilience assessments (RRA) and certify to EPA that these assessments have been completed.

The RRA must include "electronic, computer, or other automated systems (including the security of such systems)." Community water systems (CWSs) can contract the assessments to a third party that uses the EPA's Water Sector Evaluation Program, or a community can conduct their own assessments using EPA's free Water Cybersecurity Assessment Tool.

In February, 2024, the National Rural Water Association (NRWA) and WaterISAC, an international water and wastewater system security network, announced a partnership to educate small, rural utilities serving fewer than 3,300 on cybersecurity issues and cyber resilience, covering approximately 25,000 NRWA members.

In addition to EPA's resources, CISA and AWWA have introduced free services and programs to strengthen cybersecurity practices for water systems and make the implementation of cybersecurity more mainstream. AWWA is advocating that the EPA develop a regulatory entity for cybersecurity in the water sector, modeled after that of the energy sector, that would "develop, implement, and enforce cybersecurity risk and resilience requirements responsive to the cyber threats and needs of drinking and wastewater systems."

In April 2024, Congressional representatives proposed the Water Risk and Resilience Organization Act, which would create an entity to work alongside the EPA to develop cybersecurity enforcement measures for water and wastewater systems. This proposed bill follows feedback and concerns from government and nonprofit entities like the EPA and American Water Works Association (AWWA) about increased incidence of cybersecurity breaches of US water systems from foreign entities.

Funding Cybersecurity Improvements

Most of the existing funding opportunities for water and wastewater infrastructure do not currently cover cybersecurity directly, and most of the available cybersecurity services for water systems are offered for free. EPA's webpage on cybersecurity for water and wastewater systems includes a contact form to sign up for technical assistance.