PUBLIC HEALTH DIVISION
Drinking Water Services

Oregon Health Authority

800 NE Oregon St.
Portland, OR 97232-2162
Phone 971-673-0405
Fax 971-673-0694
www.healthoregon.org/dws

Cybersecurity Guidance for Oregon Public Drinking Water Systems

By Chantal Wikstrom

Given the potential for cyberattacks on water systems across the United States, Oregon drinking water providers are encouraged to actively monitor their computers and automated control systems for unusual and suspicious activity.

Notable cybersecurity incidents

- Oldsmar, FL: Hackers breached the computer and automated control systems and altered the sodium hydroxide dose from 100 ppm to 1,100 ppm. The operator noticed the changes, corrected the dosage rate and notified law enforcement. This incident happened due to unsecured remote desktop viewing, the outdated Windows 7 operating system, and poor password security.
- Ellsworth, KS: A disgruntled ex-employee of a water system was recently charged with attempting to hack the computer system to alter disinfection procedures and harm public health.

Potential cybersecurity impacts on drinking water providers

- Interruption of treatment, disinfection, and other processes
- Alarms overridden, pumps and other equipment disabled
- Theft of customer or water system employee personal data
- Access to critical locations
- Email system compromised
- Damage to system components
- Loss of telecommunications
- Loss of control systems for remote monitoring or automated treatment and distribution processes
- Water system’s ability to provide safe drinking water and protect public health is compromised

What can water systems do?

Risk assessment

- The more “connected” a system is, the more vulnerable it becomes to potential cyberattacks.
- Assume cyberattacks will be attempted and protect your public water system.
- Identify all critical IT systems, process controls, communication systems, and personnel and coordinate cyber-related duties.
- Use the AWWA Water Sector Cybersecurity Tool (login required to access this tool) to conduct the self-assessment questionnaire. Use this tool in conjunction with the AWIA (America’s Water Infrastructure Act) Risk and Resilience Assessment and Emergency Response Plan.

Actions and considerations

- Review and update your system’s Risk & Resilience Assessment and Emergency Response Plan to address cybersecurity. Include potential impacts on operations and when and how to report cybersecurity incidents. Based on findings and needs, identify potential funding opportunities.
- Update software and passwords regularly. Use anti-virus software, spam filters and firewalls.
- Consider using multi-factor authentication.
- Train all employees on proper usage and work with IT consultants to assess potential weaknesses.

When to report cybersecurity incidents

- When there is a loss of system controls or monitoring data
- When there is an impact to critical infrastructure, core functions, economic or national security, or public health
- When there is evidence of unauthorized access to critical information systems

Funding options

- USDA Rural Development Funds
- USDA Technical Assistance & Training Grants

Resources

- AWWA Free Training for Small Water Systems
- AWWA Cybersecurity Risk & Responsibility in the Water Sector
- AWWA Water Sector Cybersecurity Risk Management Guide
- EPA Water Sector Cybersecurity Brief for States
- EPA Cybersecurity Incident Action Checklist
- Water ISAC 15 Cybersecurity Fundamentals for Water Utilities

Chantal Wikstrom is a Natural Resource Specialist 3 in Drinking Water Services. Contact her at 971-666-8512 or chantal.t.wikstrom@oha.oregon.gov.