Public Water System Advanced Cybersecurity

Public water systems run operational technology (OT) and information technology (IT) systems that can be vulnerable to cyberattacks. The higher the complexity of the water system, the more areas must be protected against possible attacks. For an introduction to best practices, see Rhode Island Department of Health's factsheet *Public Water System Cyber Hygiene Basics*.

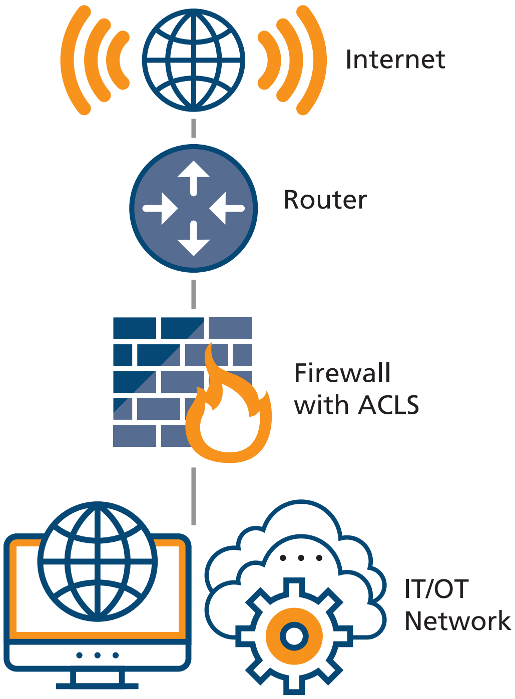
Information and Operational Technology Inventories

A public water system should have a complete inventory of its use of OT and IT. OT includes industrial control systems (ICS), such as the supervisory control and data acquisition (SCADA) systems. IT includes databases that house customer and employee information.

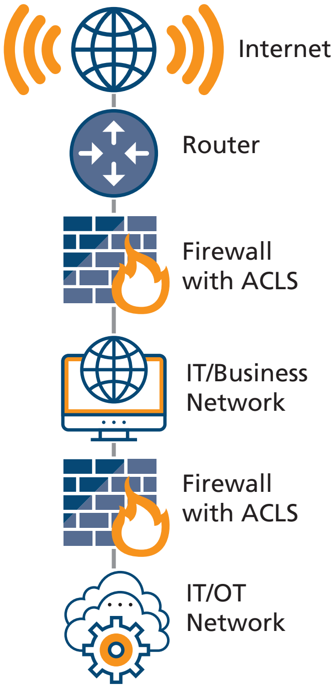
Replace Network Airgaps with Segmentation

Some public water systems may have IT and OT systems that are separated by "airgaps." Connecting IT and OT systems can have significant operational efficiencies and cost savings. To protect connected IT and OT systems, use network segmentation – a security practice that divides IT and OT systems.

Non-Segmented Network



Segmented Network



A segmented network uses firewalls to protect connected OT and IT systems.

Questions? Contact the Center for Drinking Water Quality by calling **401-222-6867** or emailing **DOH.RIDWQ@health.ri.gov** or visit us online at **health.ri.gov/PWSprepare**

Updated September 2024

Use Secure Website Domains

Gov domains are available to eligible organizations for free and are trusted domains that can help prevent against impersonation. Switch from a .org or .com to a .gov when possible.
Learn more: https://get.gov/domains/eligibility/

Complete Risk and Resilience Assessments

Community water systems serving more than 3,300 people must prepare or revise risk and resilience assessments and certify to the Environmental Protection Agency that this work has been completed every five years. All water systems can reduce their risk from cyber threats by completing the assessments and taking follow-up actions.
Learn more: www.epa.gov/waterresilience/cybersecurity-assessments

Create an Acceptable Use Policy

Water systems should prepare employees for on-the-job use of computers and other electronics with an Acceptable Use Policy (AUP). Key elements of an AUP include: general use and ownership, security, definitions of unacceptable uses (network and system-wide, email, and when using social media or websites), and an explanation of how AUP compliance will be enforced.

Implement Endpoint Protection

Cyber actors use techniques that can be difficult to detect and protect against to bypass endpoint security controls and launch attacks on target devices. Endpoint and detection response tools can help effectively protect against malicious cyber actors by employing intrusion detection and prevention systems, using signatures, conducting penetration testing, vulnerability scanning, and using cloud service provider tools to detect overshared storage and abnormal access.

RHODE ISLAND DEPARTMENT OF HEALTH

Questions? Contact the Center for Drinking Water Quality by calling **401-222-6867** or emailing **DOH.RIDWQ@health.ri.gov** or visit us online at **health.ri.gov/PWSprepare**

Updated September 2024