WATER ISAC | TOP ACTIONS to Enhance Your Utility's Cybersecurity

1 Plan for Incidents, Emergencies, and Disasters

- **Why this is important:** Regardless of utility size, the inability to promptly and efficiently contain, mitigate, and communicate about cybersecurity incidents, emergencies, or disasters could result in significant operational disruption.
- **Resource:** Incident Response Guide for the Water and Wastewater Sector

2 Minimize Control System Exposure

- **Why this is important:** Unidentified connections into the OT network present unnecessary risk to availability, control, and safety of industrial automation and control systems.
- **Resource:** Get your Stuff Off Search. Know What Your Adversaries Know!

3 Create a Cyber Secure Culture and Protect from Insider Risks

- **Why this is important:** Cybersecurity is a shared responsibility among all staff. Every employee, executive, and board member is accountable for the overall cybersecurity posture of an organization. Creating a cyber secure culture relies on leadership support and staff engagement that can result in a significant risk reduction against insider threats and risks.
- **Resource:** OUCH! Newsletters - SANS

4 Implement System Monitoring for Threat Detection and Alerting

- **Why this is important:** While many of the cybersecurity fundamentals in this publication are developed with prevention in mind, in this "assume breach" world, we must be able to detect suspicious and nefarious activity. Without the ability to detect threats within your environments, adversaries will go unnoticed.
- **Resource:** The Five ICS Cybersecurity Critical Controls

5 Account for Critical Assets

- **Why this is important:** By identifying, inventorying, classifying, and documenting the *most critical ICS/OT assets,* utilities can prioritize and allocate security resources effectively to protect those assets from potential threats, attacks, or failures that could disrupt operations or cause safety incidents.
- **Resource:** Creating an OT Asset Inventory – Dale Peterson

6 Enforce Access Control

- **Why this is important:** Maintaining strict access controls play a crucial role in protecting resources, data, and systems from unauthorized access, ensuring confidentiality, integrity, availability, and safety. Access controls should be enforced for users and devices.
- **Resource:** Implementing Phishing-Resistant MFA - CISA

>>>

7 Embrace Risk-Based Vulnerability Management

- **Why this is important:** Vulnerability management across OT and IT is essential for water and wastewater utilities in maintaining operational continuity, protecting critical infrastructure, and mitigating the risks associated with cyber threats in increasingly interconnected industrial systems.
- **Resource:** The OT Vulnerability Management Handbook

8 Secure the Supply Chain

- **Why this is important:** Engaging with third-party vendors expands a utility's attack surface whereby cyber threats can infiltrate a utility through its supply chain. Likewise, as third parties often have access to sensitive data/information, this necessitates regular assessments of third-party security postures.
- **Resource:** NIST Cybersecurity Framework 2.0: Quick-Start Guide for Cybersecurity Supply Chain Risk Management (C-SCRM)

About WaterISAC

WaterISAC is the only all-hazards security information source for the water and wastewater sector. We serve over 3,800 water sector personnel across several hundred utilities and other organizations. Our utility members provide water and wastewater service to most of the United States, and we also serve utilities in Canada, Australia, and New Zealand. Find out more about WaterISAC's products and services here.