

October 2026

Priority Level: High

Threat Overview: Water, Waste Water And Energy Production

In recent months traditional threat actors and nation state threat actors have been increasing their attacks on Supervisory Control and Data Acquisition (SCADA) & Industrial Control Systems (ICS) targeting Water, Waste Water and Energy production industries. These attacks primarily target small organizations due to the impact attacks can have on water, waste water, and energy production. Every organization regardless of size is a target. Every organization is being scanned continuously for potential attack paths. The good news is there are steps you can take as an organization to improve your cybersecurity posture, starting with basic practices.

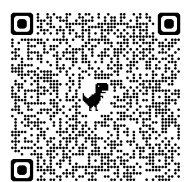
Threats to Industrial Systems

- **Default and Weak Passwords:** It is common for successful Operational Technology (OT) attacks to use default, weak, or commonly used passwords.
- **Monitoring and Response:** Achieving full visibility into your operational networks allows for quicker detection and response to emerging threats. Device logs should go to a centralized storage location. Log monitoring and correlation can help reduce the odds an attack goes undetected.
- **Unpatched or Legacy Systems:** In many cases, devices can go unpatched for the entirety of their lifecycle. The case may also be there are no available patches due to the age of the device or the vendor becoming defunct or ending support.
- **Inadequate Network Isolation:** Not having adequate network isolation allows attackers to pivot between devices or networks. This allows attackers to gain access to a wider environment that they can perform additional attacks within. You may find that your network equipment may not provide the level of security you need to protect your environment.

GOAL: The goal of this campaign is to give business leaders, IT teams, and employees simple, actionable guidance to strengthen defenses against modern cyber threats. While attackers continue to use increasingly sophisticated methods, many successful intrusions still exploit basic weaknesses. Strong authentication, patching, access control, secure backups, employee awareness, and incident response planning can make a significant difference in reducing risk and keeping businesses resilient.

Remember: Security is a Shared Responsibility

- ✓ When in doubt, verify through official internal channels before interacting with unexpected requests.
- ✓ If you click on a suspicious link or enter credentials on a suspicious website, notify your security operations center or responsible IT support immediately.



For more information, scan the QR code or visit
ransomwareinfo.oregon.gov



CYBER READINESS TIPS

Best Practices For Organizations

- **Require MFA** for email, remote access, administrative accounts, and other important business systems.
- **Apply security updates and patches promptly** to operating systems, applications, browsers, network devices, and OT.
- Give employees and vendors only the access they need, and **regularly review accounts and permissions**.
- **Maintain secure backups** of important data and systems, and regularly test your ability to recover.
- **Monitor network activity continuously**. Log monitoring and correlation can generate automated alerts for anomalous or suspicious activity.

Cyber Risk Visibility

- Ask your IT staff or provider for a report that includes **metrics regarding the cyber risk** your organization faces.
- **Information you see on the report** should be actionable and easy to understand.
- Ask yourself **how often should the report be generated?**
- **Consider the audience** of this report and whether you may need reports for different levels of leadership. An executive may want different information than an IT manager.
- **Is your organization tracking** sector-specific cyber threats, and is this intelligence actively integrated into your reporting?

Questions For Organizations



- **Is MFA enabled** for critical accounts?
- Are our systems and applications **patched and up to date?**
- Do we regularly **review user and vendor access/activity logs?**
- How do we **ensure separation between IT and OT networks** within our organization?
- Does our IT staff **know how and when to contact operational staff?**
- Do we have an **incident response plan?** What are we doing to test and improve it?
- Can we **detect and isolate compromised devices?**

If You Think You Are Compromised

- Quickly **establish joint communications** between IT staff and operational staff.
- Determine if the outage is being caused by a **cyber attack or a device failure**.
- **Monitoring alerts** could potentially identify that the failure is the result of a cyber attack before physically inspecting the device.
- Look for **anomalous behavior** in your network and attempt to provide context to the overall health of your network.
- **Compare current configuration** with expected configurations.

Additional Resources:

Oregon Emergency Response System
(OERS) 1-800-452-0311

Cybersecurity & Infrastructure Security Agency (CISA)
888-282-0870 | www.cisa.gov

FBI Field Office - Cyber Task Forces
Portland Office 503-224-4181
<https://www.ic3.gov/fbi.gov/contact-us/field>

Multi-State Information Sharing and Analysis Center®
(MS-ISAC®) 866-787-4722

State of Oregon Security Operations Center
503-378-5930 | css.soc@eis.oregon.gov

National Institute of Standards and Technology (NIST)
<https://www.nist.gov/cybersecurity-and-privacy>



For more information on strengthening your cybersecurity posture, refer to the FBI's Operation Winter SHIELD guidance.
<https://www.fbi.gov/investigate/cyber/wintershield>

