

October 2026

Priority Level: High

Threat Overview: Operational Technology

Threat actors are actively targeting Operational Technology (OT) devices in sophisticated attacks against State, Local, Tribal, and Territorial (SLTT) organizations. This technology includes Programmable Logic Controllers (PLCs), Remote Terminal Units (RTUs), Human-Machine Interfaces (HMIs), Internet of Things (IoT), and more. These devices can be leveraged to deny access and conduct other attacks against industrial equipment, critical infrastructure control and monitoring capabilities, Heating, Ventilation, and Air Conditioning (HVAC), informational displays, and many other systems. In recent months these attacks have become more frequent and have been conducted by nation-state threat actors, hackers, and cybercriminal groups.

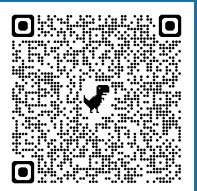
Threat Vectors to Watch

- **Default & Weak Passwords:** It is common for successful OT attacks to use default, weak, or commonly used/reused passwords.
- **Inherently Vulnerable Devices:** Attackers commonly leverage zero-day vulnerabilities to gain access to vulnerable OT devices. Hard-coded vendor/communication access and default credentials are often used to allow vendor access to the device - this practice is often out of the control of IT and OT operators.
- **Unpatched or Legacy Systems:** In many cases devices can go unpatched for the entirety of their lifecycle. There may be no patches available 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 operational staff simple, actionable guidance to strengthen defenses against modern cyber threats. While attackers use complex and evolving methods, many successful intrusions still exploit basic weaknesses. The foundational controls show that doing the simple things, such as patching, authentication, access control, visibility, and backup, can make a biggest difference. More awareness materials will follow through October's Cybersecurity Awareness Month.

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

- **Implement security controls**, such as vulnerability management, advanced threat detection systems, and network segmentation.
- **Continuously monitor** systems and networks for any signs of malware or suspicious activities.
- **Discontinue use of legacy devices** where possible, this greatly reduces the risk associated with unsupported devices in your environment.
- **Use strong passwords** for all OT devices, and change passwords routinely. If you have a low character limit for supported passwords use randomized passwords where possible.
- **Stay up-to-date** on cybersecurity news affecting your OT devices. A good source for this would be the CISA Known Exploited Vulnerabilities and Industrial Control Systems.

Questions For Organizations

- Do we have complete **discovery of all devices** on each of our networks?
- What are we doing to make sure **unsupported devices** are replaced with modern devices?
- How are we ensuring **proper network isolation**?
- What are our **password complexity** requirements?
- How often are we **rotating passwords**?
- What are we doing to ensure we don't have any **default passwords** in our environment and how often is this performed?
- How are we ensuring our **devices are updated**?

Cyber Risks 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?

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 cyber 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>

