CyberOhio

CyberOhio

Water Operators Cyber Risks, Responsibilities

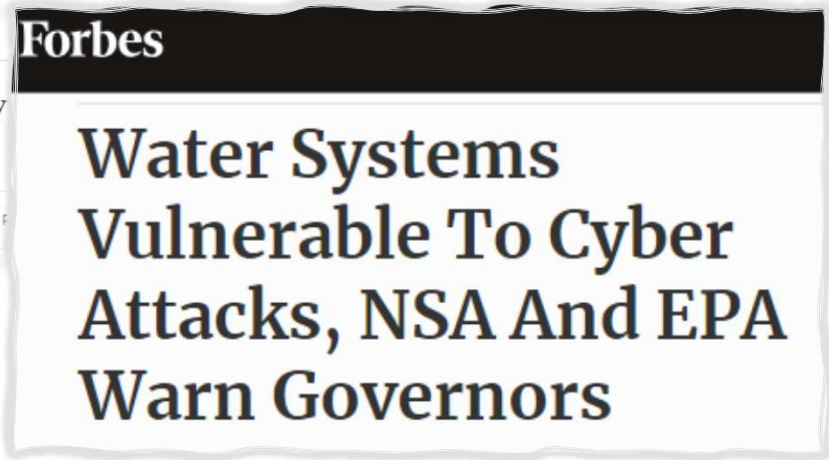
And Resources to Assist

Southwest Ohio Water Environment Association Seminar
November 21, 2024

Agenda

- Why Cybersecurity Matters
- Overview of CyberOhio
- Federal Critical Infrastructure Cyber Priorities
- Assessing Your Operations and Network
- State of Ohio Cyber Assistance
- Federal Assistance and Resources

WHY CYBERSECURITY MATTERS FOR WATER OPERATORS



WHY CYBERSECURITY MATTERS

Cybersecurity is an issue of public trust, national security, and fiscal responsibility. It is imperative that we protect citizens and prevent critical service disruption.

The average time to recover from ransomware attacks rose in nearly every sector last year. In 2021, the average recovery time for all sectors was just over a week. 2022 saw an increase in the average recovery time from 7.8 days in 2021 to 14.9 days in 2022 or a 91% increase. The energy and technology sectors saw a 54% uptick.

Ransomware is one of the biggest threats today. Black Kite's 2023 Ransomware Landscape Report reports that ransomware victims nearly doubled between April 2022 and 1.6 times higher than the peak month in 2022.

Cyber-attacks are frequent. Global cyber-attacks rose by 7% in Q1 2023. Weekly cyber-attacks have increased worldwide by 7% in Q1 2023 compared to the same period last year. Overall, global cyberattacks increased by 38% in 2022 compared to 2021.

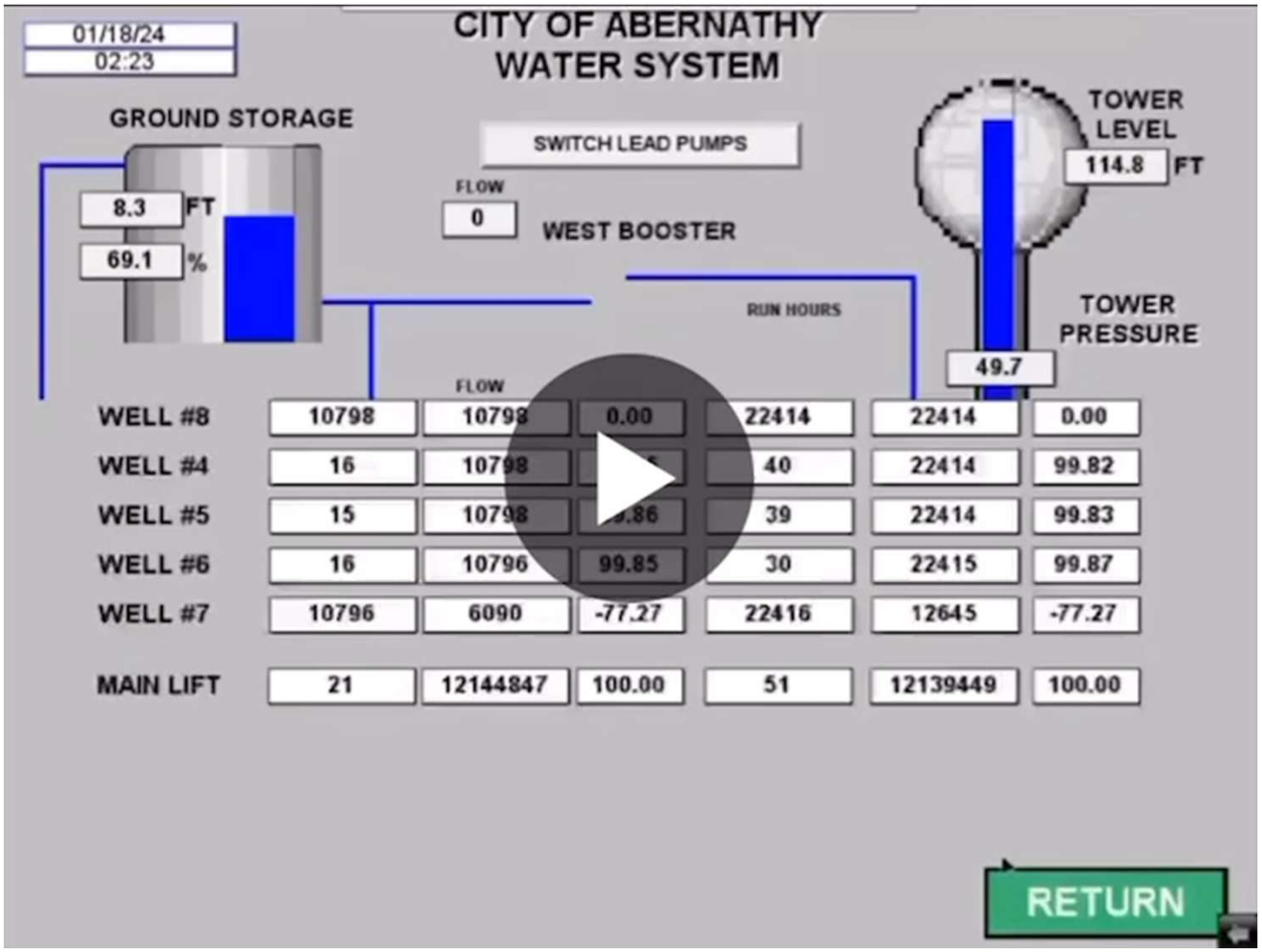
Attacks are becoming more complex. 59% of the public sector saw increased volume and complexity of attacks, with 21% of public sector organizations taking an average of a month to recover. Source: Microsoft Digital Crimes Report.

In 2023, the global annual cost of cybercrime is predicted to top $8 trillion. In 2021, U.S. financial institutions lost nearly $1.2 billion in costs due to ransomware attacks alone, representing an about 200% increase over the previous year.


UNITRONICS
YOU HAVE BEEN
HACKED
DOWN WITH ISRAEL
الموت لإسرائيل
EVERY EQUIPMENT
"MADE IN ISRAEL"
IS CYBER AV3NGERS
LEGAL TARGET
F1
F2
F3
F4
ESC
V350

TLP:Clear

Example of Attack to SCADA



CYBEROHIO BACKGROUND

CyberOhio was initially created by Attorney General Mike DeWine as a Small Business Cybersecurity Advisory Board in 2017

CyberOhio became an initiative of InnovateOhio at the beginning of the DeWine-Husted Administration and continued its work as an advisory board.

In 2022, Executive Order 2022-07D created the Cybersecurity Strategic Advisor (CSA) and tasked them with four core missions: protecting the base, assisting locals, bolstering the workforce, and securing critical infrastructure.

CyberOhio evolved into a broader initiative of the Governor's Office to aid the CSA in the execution of the duties laid out in the EO.

CyberOhio and the CSA coordinate all cybersecurity activities within the State of Ohio.

CyberOhio and the CSA were created because the DeWine-Husted administration prioritizes cybersecurity.

FOUR MISSIONS MAPPED TO EO 2022-07D

Coordinate a "…unified approach among state agencies to guide the state's cyber initiatives…"

Protect State systems and information	Support Ohio's local government cybersecurity efforts	Address cybersecurity workforce challenges	Engage the private sector in statewide efforts of cyber protection activities
Protect the Base	**Assist Local Governments**	**Cyber Workforce**	**Critical Infrastructure Cyber**

Whole-of-State Approach

CRITICAL INFRASTRUCTURE CYBERSECURITY

CyberOhio aims to assist public and private critical infrastructure partners with securing their systems. CyberOhio's CI focus includes:

Water and Wastewater Systems	Energy	Critical Communications & PSAPs	Emergency Services	Elections	Transportation

Notice of Proposed Rule Making under CIRCIA – Critical Infrastructure Incident Reporting Rules.

U.S. EPA Water Infrastructure Cybersecurity 2023 – Current.

January 2023, the President's National Cyber Strategy makes critical infrastructure protection a top priority.

CyberOhio is working with various State Agencies to uplift Ohio's critical infrastructure cybersecurity preparedness.

REGULATION IS COMING:
CIRCIA INFRASTRUCTURE BREACH REPORTING

- In March 2022, President Biden signed into law the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA).
- On March 25, 2024, CISA published a draft Cyber Incident Reporting Notice of Proposed Rule Making. The comment period is 60 days.
- CISA will issue a Final Rule within 18 months of the NPRM.
- Once the CIRCIA Regulation is Final, Covered Organizations will be required to report all covered events to CISA.

WHAT CYBER EVENTS ARE REPORTABLE UNDER PROPOSED CIRCIA REGULATION?

- Only “Substantial covered cyber events should be reported to CISA. But, “substantial” is relative and broad.
- These are events that meet one or more of the following impacts:

- Impact 1: Substantial Loss of Confidentiality, Integrity, or Availability
- Impact 2: Serious Impact on Safety and Resiliency of Operational Systems and Processes.
- Impact 3: Disruption of Ability to Engage in Business or Industrial Operations.
- Impact 4: Unauthorized Access Facilitated or Caused by Third Party (MSP, Data Hosting, Supply Chain).

CIRCIA INFRASTRUCTURE BREACH REPORTING REGULATION

According to CISA NPRM:

- All Critical Infrastructure Owners and Operators and Federal, State, Local, Territorial, and Tribal Government Partners will report cyber attack information.
- 72-Hour Notification from event discovery. Supplement as needed with additional forms.
- The definition of what constitutes a "substantial cyber incident" is very broad.
- Noncompliance can result in civil enforcement by the US Justice Dept.

What types of activity should be shared:

- Unauthorized access to your system
- Denial of Service (DOS) attacks that last more than 12 hours
- Malicious code on your systems, including variants if known
- Targeted and repeated scans against services on your systems
- Repeated attempts to gain unauthorized access to your system
- Email or mobile messages associated with phishing attempts or successes
- Ransomware against Critical Infrastructure, including variant and ransom details if known

US EPA WATER INFRASTRUCTURE CYBERSECURITY

In early 2023, the US EPA announced in a letter ruling, reinterpreting the U.S. Clean Water Act, that state environmental agencies must assess the cybersecurity of water and sanitary wastewater treatment plants. As a result:

- Ohio EPA began developing a strategy to meet this requirement.
- Letter Ruling was rescinded by US EPA in early Fall 2023, due to legal action by several states, local governments, and the industry.
- Expect formal NPRM in the near future.
- March 2024, White House and US EPA sent a letter to all State Governors and State EPA Administrators – requesting plans on addressing cyber risk to water and wastewater operations.
  - Most states, including Ohio, provided a plan of action regarding their covered entities at the end of June 2024.

ENFORCEMENT IS COMING: US EPA ENFORCEMENT ALERT

On May 20, the U.S. EPA issued an enforcement alert citing growing cybersecurity threats and vulnerabilities to community drinking water systems and laying out the steps needed to comply with the Section 1433 of the Safe Drinking Water Act.

EPA will increase the number of planned inspections and take civil and criminal enforcement actions, in response to cases of imminent and substantial endangerment.

EPA, CISA AND FBI RECOMMEND THE FOLLOWING STEPS:

- Reduce exposure to public-facing internet.
- Conduct regular cybersecurity assessments.
- Change default passwords immediately.
- Conduct an inventory of OT/IT assets.
- Develop and exercise cybersecurity incident response and recovery plans.
- Backup OT/IT systems.
- Reduce exposure to vulnerabilities.
- Conduct cybersecurity awareness training.

OHIO EPA – FOCUS ON EMERGENCY RESPONSE AND RECOVERY

Under existing law, community public water systems must have a contingency plan for dealing with emergencies. Ohio focuses on incident response and recovery of operations.

Emergencies include malicious acts and cyber security incidents.

Plan requirements focus more on response to a threat and ensuring that water can continue to be provided.

- Identify alternate sources of water and be able to provide 1 gallon per person per day in the event of an emergency.
- Systems to test their ability to run on emergency power and manually on a monthly

NATIONAL SECURITY MEMORANDUM ON IMPROVING CYBERSECURITY FOR CRITICAL INFRASTRUCTURE

- CISA, NIST and other agencies are working to develop baseline cybersecurity performance goals consistent across all critical infrastructure (CI) sectors.
- These voluntary, cross-sector Cybersecurity Performance Goals (CPGs) establish a common set of fundamental cybersecurity practices for CI, particularly small- and medium-sized organizations.
- The CPGs prioritize a subset of IT and operational technology (OT) cybersecurity practices that CI owners and operators can implement to reduce the likelihood and impact of known risks.
- **The CPGs are intended to be:**

  A baseline set of cybersecurity practices applicable across critical infrastructure with known risk-reduction value.

  A benchmark for to prioritize, measure and improve IT and OT cybersecurity maturity.

  Unique from other control frameworks. Practices that address risk to individual entities, and National risk.

- **The CPGs are:**

  Voluntary: Does not create new authorities that compel owners and operators to adopt the CPGs or provide any reporting regarding or related to the CPGs to any government agency.

  Not Comprehensive: Capture a core set of cybersecurity practices with known risk-reduction value broadly applicable across sectors.

  Supplement NIST Cybersecurity Framework (CSF) to enable focused improvements across suppliers, vendors, business partners, or customers.

BUILDING A CYBER ASSESSMENT FRAMEWORK

Why Build a Cyber Assessment Framework?

- Greater CISA and other cybersecurity regulations for critical infrastructure, especially water and wastewater, are coming. The industry should begin preparing itself now.
- It is in the interest of regional, state, and national security to work together to ensure our energy is secure from foreign cyber attack threats.

WHAT IS A CYBER ASSESSMENT FRAMEWORK ?

A cyber security assessment framework allows organizations to systematically analyze and review their digital infrastructure and operations to control and mitigate cyber security risks.

See the link below for more information:

https://www.nist.gov/cyberframework/framework

WHAT STEPS SHOULD WATER OPERATORS TAKE TO BUILD AN ASSESSMENT FRAMEWORK?

1. Build an association-based assessment framework.
2. Start with self-assessments.
3. Create and collaborate on a framework of minimum standards for water operators.
4. Utilize training resources to uplift your skills and resilience.
5. Be assessed by an outside organization.
6. Document the steps you are taking to uplift your cybersecurity. Begin preparing for mandatory incident reporting.

CURRENT OHIO COMPREHENSIVE CYBERSECURITY PLAN GOALS

- Improve cyber intelligence sharing across local, state and federal organizations
- Expand Ohio Persistent Cyber Improvement (OPCI) – 3 levels of training, cyber assessments and table-top exercises for local governments
- Whole-of-State cyber capabilities and resiliency
- Improve cybersecurity across state agencies
- Update and test the Ohio Cyber Incident Response Emergency Operations Plan with state and local governments

OHIO PERSISTENT CYBER INITIATIVE - ACTION PLAN

Complete a Cybersecurity Assessment

- Understanding what your vulnerabilities are is crucial to charting a way forward.
- Coordinate with your county to get an assessment done through the O-PCI program.

Close gaps with training and resources

- Use the O-PCI program to learn and train for preventing cyber-attacks.
- Apply for grant dollars through the Local Government Cybersecurity Grant program to fill any gaps found.

Create a response plan for a cyber-attack

- What processes do you need to have in place to function?
- Reference the State Cyber Emergency Response plan.
- Coordinate with your county EMA to create a plan specific to you

Test your plan with a tabletop exercise

- Participate in a tabletop exercise with your county through O-PCI or CISA.
- Identify further areas for improvement
- Repeat!

LOCAL GOVERNMENT CYBER GRANTS - MORE TO COME!

The Infrastructure Investment and Jobs Act (IIJA) included provisions for SLCGP (State and Local Cybersecurity Grant Program) to address cyber risks and threats to the information systems of state, local, or tribal governments. State of Ohio is matching with over $10 million in-kind contributions.

$7 million for Local Government Grants

Our initial grant program gave local government entities the software tools and services needed to continue the improvement gained through the Persistent Cyber Improvement Program.

The application window closed in September 2024.

Cyber Integration Center

Intelligence and information sharing center and Hub for State of Ohio Incident Response.

- Local government cybersecurity grants (Helps Defend and Recover)
- Local government Dot Gov Domain Transition (Protects Websites and Prevents Fraud)
- Ohio Cyber Integration Center (Cyber Intelligence and Incident Response for Local Governments)

APPENDIX – STATE AND FEDERAL RESOURCES

CYBEROHIO: ADDITIONAL CYBER RESOURCES

CyberOhio exists to connect you to resources and help you navigate the cybersecurity world.

Additional State of Ohio resources and support available:

Ohio Department of Public Safety, Department of Homeland Security - Cyber Integration Center

Ohio Adjutant General's Office - Cyber Reserve

Connect with us at:
CyberOhio@Governor.ohio.gov

FEDERAL RESOURCES FOR SECURING WATER SYSTEMS

1. Reduce Exposure to the Public-Facing Internet to reduce exposure of key assets to the public-facing Internet.
   - Free resource: CISA's Free Cyber Vulnerability Scanning for Water Utilities fact sheet explains the process and benefits of signing up for CISA's free vulnerability scanning program.
   - Free service: Email vulnerability@cisa.dhs.gov with the subject line, "Requesting Cyber Hygiene Services" for CISA Cyber Hygiene Services, which proactively identify and enable timely mitigation of internet-exposed assets.

2. Conduct Regular Cybersecurity Assessments to understand the existing vulnerabilities within OT and IT systems.
   - Free service: EPA Cybersecurity Assessments can help assess cybersecurity posture.
   - Free resources: A free CPG assessment can be administered by a CISA cybersecurity advisor CISA Regions) or through a self-assessment.

3. Change Default Passwords Immediately to strong, and complex passwords for all water systems and implement multifactor authentication (MFA) where possible.
   - Free resources: CISA's Secure our World Campaign: Use Strong Passwords and More than a Password Campaign. For additional cyber guidance, see CISA's Cyber Guidance for Small Businesses.

4. Conduct an Inventory of OT/IT Assets: Focus efforts on internet-connected devices and devices where manual operations are not possible. Monitor to identify the devices communicating on your network.
   - Free service: EPA's Cybersecurity Technical Assistance Program supports you in conducting an inventory.
   - Free tool: CISA's Malcolm tool enables network monitoring with custom parsers designed for industrial control system (ICS)/OT protocols.

FEDERAL RESOURCES FOR SECURING WATER SYSTEMS

5. Develop and Exercise Cybersecurity Incident Response and Recovery Plans
   - Free resources: EPA's Cybersecurity Action Checklist and CISA's Incident Response Plan (IRP) Basics help to develop cyber incident response plans.
   - Free tools: CISA Tabletop Exercise Package (CTEP) and EPA tabletop exercise (TTX) scenario tools assists critical infrastructure owners and operators in developing their own tabletop exercises to meet their specific needs.

6. Backup OT/IT Systems: Test backup procedures, ensure good backup files, and isolate backups from network connections.
   - Free resources: CISA's Cyber Essentials Toolkit Chapter 5: Your Data provides guidance on backing up your systems.

7. Reduce Exposure to Vulnerabilities: Keep all systems up to date with patches and security updates. Prioritize OT patches in accordance with CISA's Known Exploited Vulnerabilities (KEV) catalog during scheduled downtime of OT.

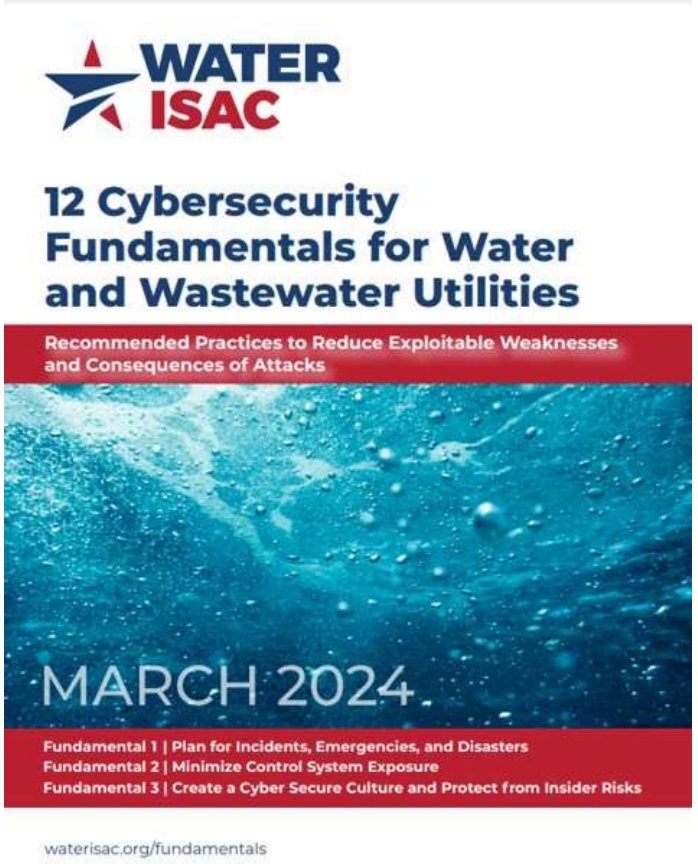
8. Conduct Cybersecurity Awareness Training Annually to help all employees understand the importance of cybersecurity and how to prevent and respond to cyberattacks.
   - Free resources: See EPA Cybersecurity Training and CISA's free Industrial Control Systems cybersecurity virtual training to learn how to protect against cyberattacks to critical infrastructure.

Visit CISA's Water and Wastewater Systems Cybersecurity and EPA's Cybersecurity for the Water Sector webpages for more information and resources. Also, visit the American Water Works Association's (AWWA's), the WaterISAC, and MS-ISAC for additional resources related to cybersecurity and CI.

WATER ISAC:
12 CYBERSECURITY FUNDAMENTALS

1. Plan for Incidents, Emergencies, and Disasters
2. Minimize Control System Exposure
3. Create a Cyber Secure Culture and Protect from Insider Risks

- Waterisac.org/fundamentals



QUESTIONS?

OHIO.ORG

Ohio THE HEART OF IT ALL™

CYBEROHIO

KIRK HERATH

Cybersecurity Strategic Advisor to Governor Mike DeWine

Chair, CyberOhio

- Kirk Herath is Governor Mike DeWine and Lt. Governor Jon Husted's Cybersecurity Strategic Advisor and Chairman of CyberOhio, the State of Ohio's Cybersecurity Advisory Board.
- His role spans coordinating and enhancing the State of Ohio's cybersecurity capabilities, working with local governments to prepare and remediate cyber attacks, and helping to build a modern cyber workforce.
- He retired as Vice President, Associate General Counsel, and Chief Privacy Officer for Nationwide after 32 years.
- Kirk is Past President and past board member of the International Association of Privacy Professionals, and he served on the U.S. Department of Homeland Security's Data Privacy and Integrity Advisory Committee from 2005 to 2011. Kirk is admitted to the Ohio Bar.