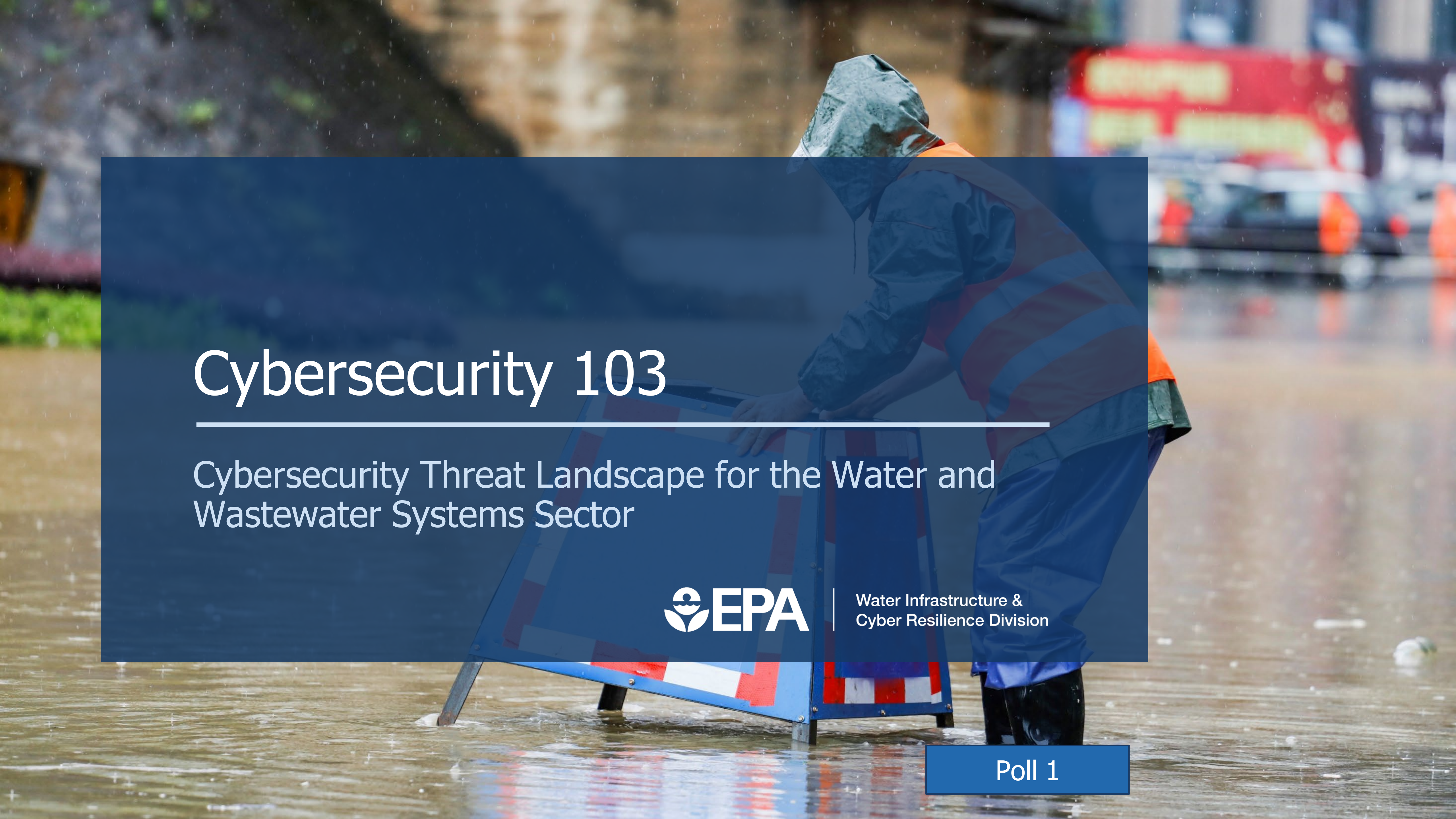


Cybersecurity 103

Cybersecurity Threat Landscape for the Water and Wastewater Systems Sector

EPA | Water Infrastructure & Cyber Resilience Division

Poll 1

Speaker

- Vijal Pancholi, Cybersecurity Analyst

- EPA’s Office of Water
    - Office of Ground Water and Drinking Water
    - Water Infrastructure and Cyber Resilience Division
    - Cybersecurity Branch

- B.S. Computer Networks
- Certified in Cybersecurity

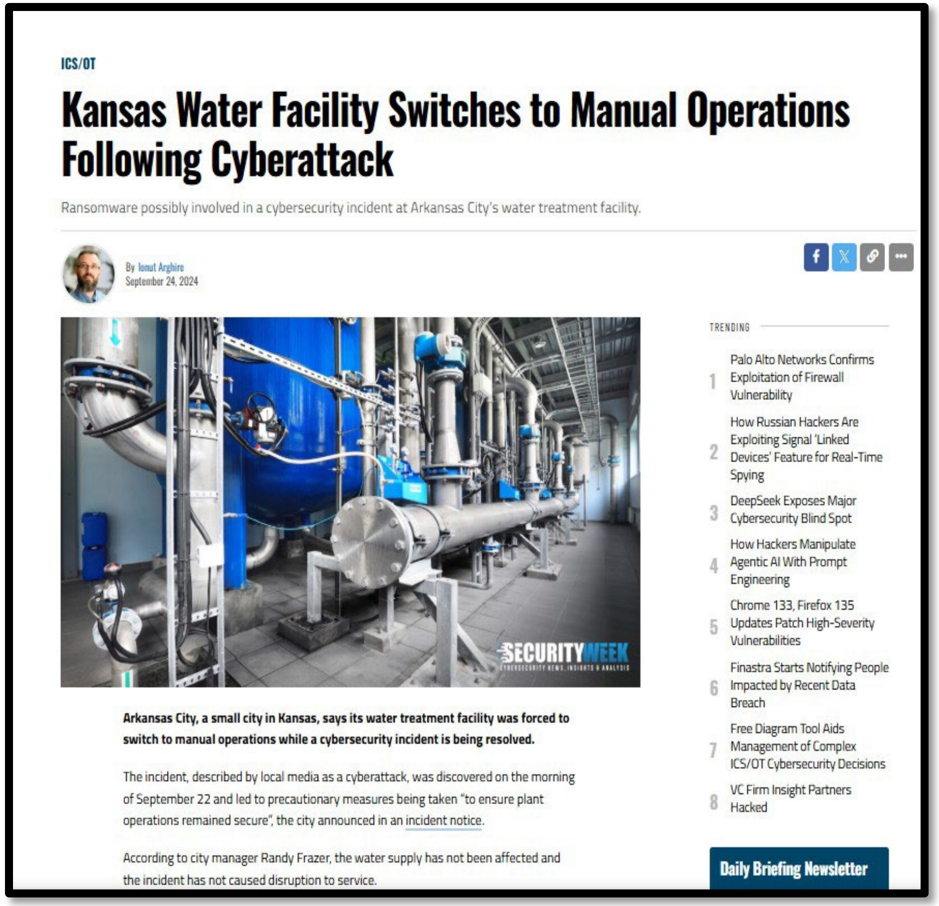
- Email: Pancholi.Vijal@epa.gov

Course Logistics and Continuing Education

- Troubleshooting
  - If you are having audio or visual trouble, please exit the course and rejoin.
  - If you continue to have trouble, please send a private chat to Melanie Woods (GDIT).
- Ways to Interact
  - Submit questions in the chat
  - Respond to poll questions
- Wrap Up and CEUs
  - At the end of the course, please complete the course evaluation.
  - Continuing education is tracked by attendance and poll responses.

The Evolving Cyber Threat Landscape

- Cyberattacks have evolved from largely IT-based ransomware to OT-focused attacks.
- Increase in frequency and severity of unauthorized remote access and ransomware attacks.
    - Many of these attacks are malware-free and target internet-exposed devices with vulnerabilities.
- Groups associated with foreign states have disrupted services at US water and wastewater utilities, resulting in operational impacts.



ICS/OT

Kansas Water Facility Switches to Manual Operations Following Cyberattack

Ransomware possibly involved in a cybersecurity incident at Arkansas City's water treatment facility.

By Ionut Arghire
September 24, 2024

Arkansas City, a small city in Kansas, says its water treatment facility was forced to switch to manual operations while a cybersecurity incident is being resolved.

The incident, described by local media as a cyberattack, was discovered on the morning of September 22 and led to precautionary measures being taken "to ensure plant operations remained secure", the city announced in an incident notice.

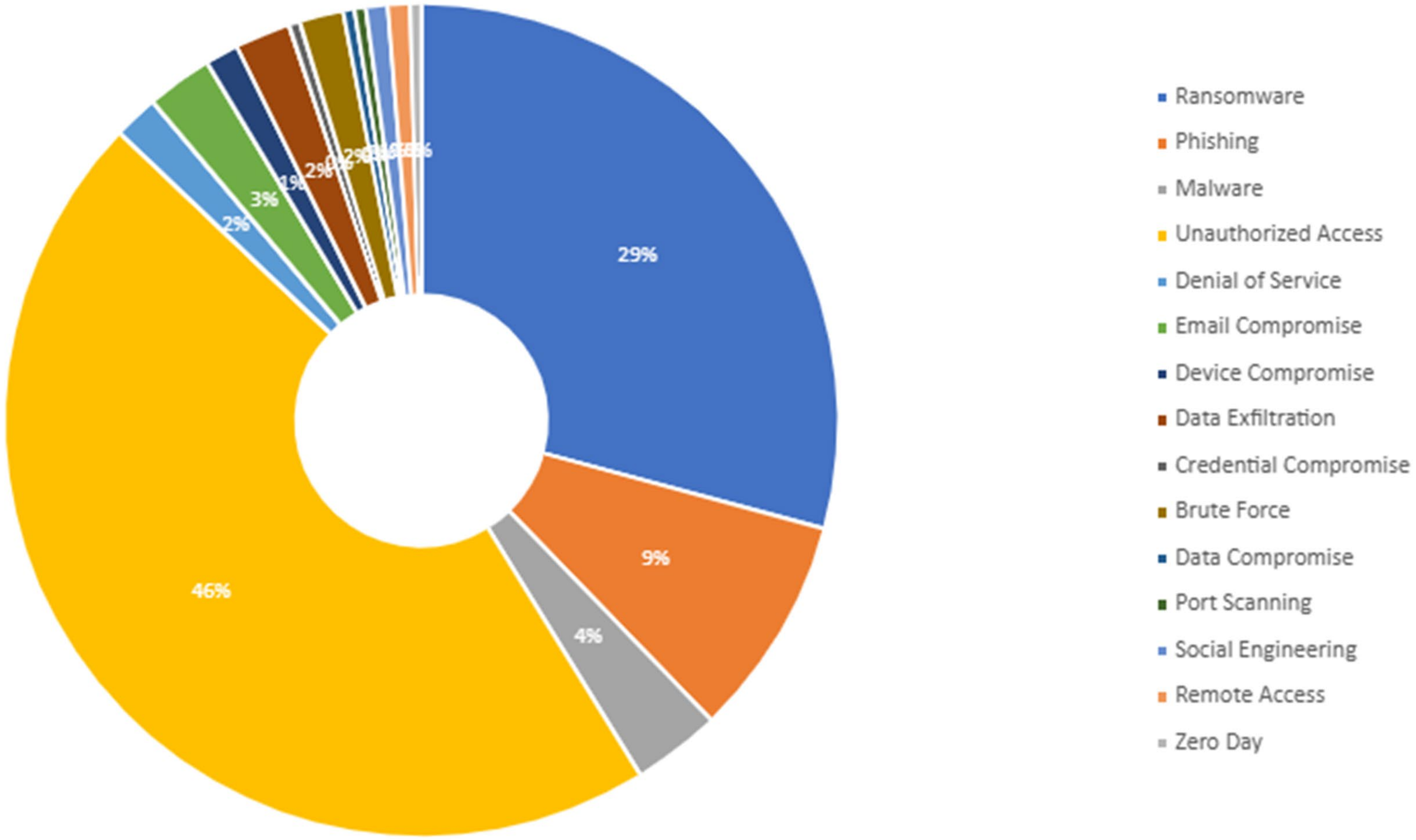
According to city manager Randy Frazer, the water supply has not been affected and the incident has not caused disruption to service.

TRENDING

1. Palo Alto Networks Confirms Exploitation of Firewall Vulnerability
2. How Russian Hackers Are Exploiting Signal 'Linked Devices' Feature for Real-Time Spying
3. DeepSeek Exposes Major Cybersecurity Blind Spot
4. How Hackers Manipulate Agentic AI With Prompt Engineering
5. Chrome 133, Firefox 135 Updates Patch High-Severity Vulnerabilities
6. Finastra Starts Notifying People Impacted by Recent Data Breach
7. Free Diagram Tool Aids Management of Complex ICS/OT Cybersecurity Decisions
8. VC Firm Insight Partners Hacked

Daily Briefing Newsletter

Water and Wastewater Cybersecurity Incidents



AGENDA

1) Big Picture: Cyber Threats to Critical Infrastructure
2) State-Sponsored Cyber Threats
3) Targeting of ICS/SCADA Devices
4) Malware
5) Human-Machine Interface Threats
6) Other Examples of Cybersecurity Threats & Incidents at Water Systems
7) Stay Informed
8) Cybersecurity Incident Reporting
9) Cybersecurity Resources
10) Wrap-Up

Big Picture: Cyber Threats to Critical Infrastructure

Big Picture: Cyber Threat Landscape

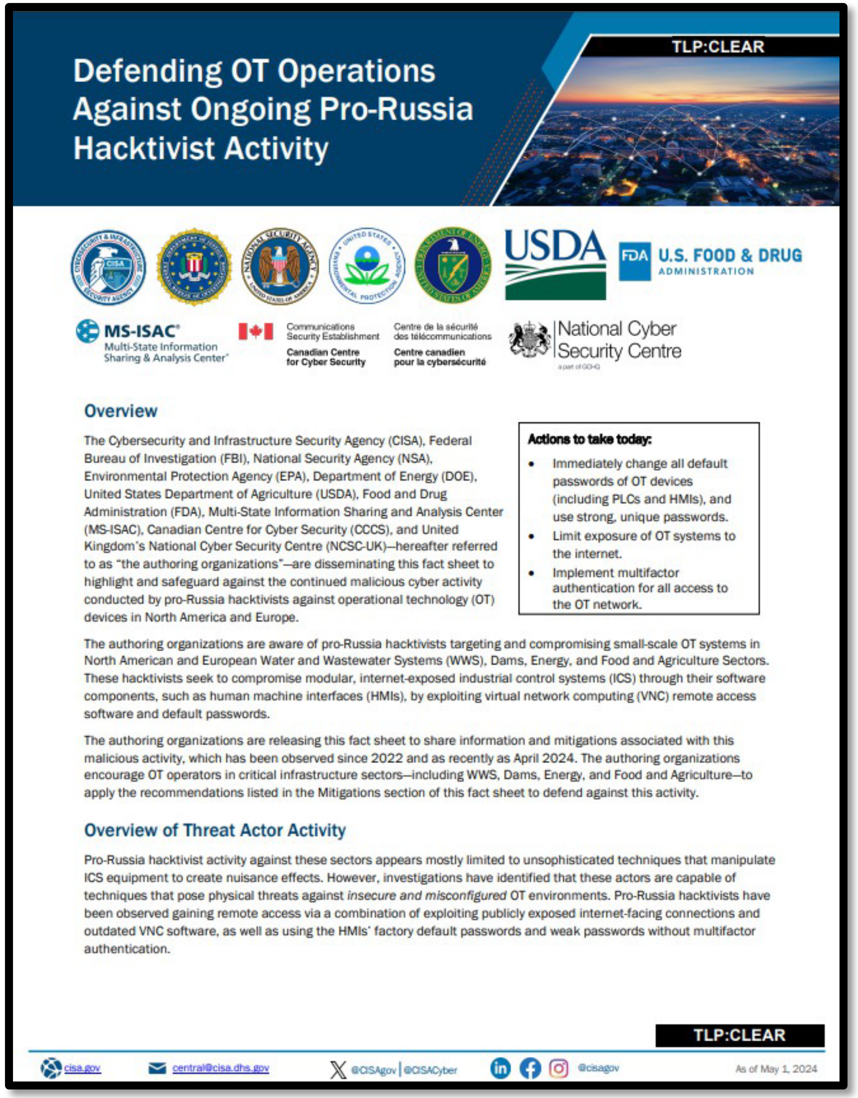
Threats to Critical Infrastructure Organizations and Industrial Control Systems (ICS)

- State-Sponsored Cyber Actors (e.g., Russia, PRC, Iran)
- Advanced Persistent Threat (APT) Cyber Tools Targeting ICS/SCADA Devices
- Known Exploited Vulnerabilities (Information Technology (IT) and Operational Technology (OT))
- Third-Party Risks
- Cyber Threats to & Incidents at U.S. Water and Wastewater Utilities

State-Sponsored Cyber Threats

Pro-Russia Threat Actor: CARR

- Remote access gained through publicly exposed internet connections, factory default and weak passwords, and lack of multifactor authentication.
- Resulted in maxed out set points, altered settings, turned off alarms, and changed administrative passwords to lock out operators.
- Many victims reverted to manual operations.



TLP:CLEAR

Defending OT Operations Against Ongoing Pro-Russia Hacktivist Activity

MS-ISAC Multi-State Information Sharing & Analysis Center

Communications Security Establishment Canadian Centre for Cyber Security

Centre de la sécurité des télécommunications Centre canadien pour la cybersécurité

National Cyber Security Centre a part of GCHQ

Overview

The Cybersecurity and Infrastructure Security Agency (CISA), Federal Bureau of Investigation (FBI), National Security Agency (NSA), Environmental Protection Agency (EPA), Department of Energy (DOE), United States Department of Agriculture (USDA), Food and Drug Administration (FDA), Multi-State Information Sharing and Analysis Center (MS-ISAC), Canadian Centre for Cyber Security (CCCS), and United Kingdom's National Cyber Security Centre (NCSC-UK)—hereafter referred to as "the authoring organizations"—are disseminating this fact sheet to highlight and safeguard against the continued malicious cyber activity conducted by pro-Russia hacktivists against operational technology (OT) devices in North America and Europe.

Actions to take today:

- Immediately change all default passwords of OT devices (including PLCs and HMIs), and use strong, unique passwords.
- Limit exposure of OT systems to the internet.
- Implement multifactor authentication for all access to the OT network.

The authoring organizations are aware of pro-Russia hacktivists targeting and compromising small-scale OT systems in North American and European Water and Wastewater Systems (WWS), Dams, Energy, and Food and Agriculture Sectors. These hacktivists seek to compromise modular, internet-exposed industrial control systems (ICS) through their software components, such as human machine interfaces (HMIs), by exploiting virtual network computing (VNC) remote access software and default passwords.

The authoring organizations are releasing this fact sheet to share information and mitigations associated with this malicious activity, which has been observed since 2022 and as recently as April 2024. The authoring organizations encourage OT operators in critical infrastructure sectors—including WWS, Dams, Energy, and Food and Agriculture—to apply the recommendations listed in the Mitigations section of this fact sheet to defend against this activity.

Overview of Threat Actor Activity

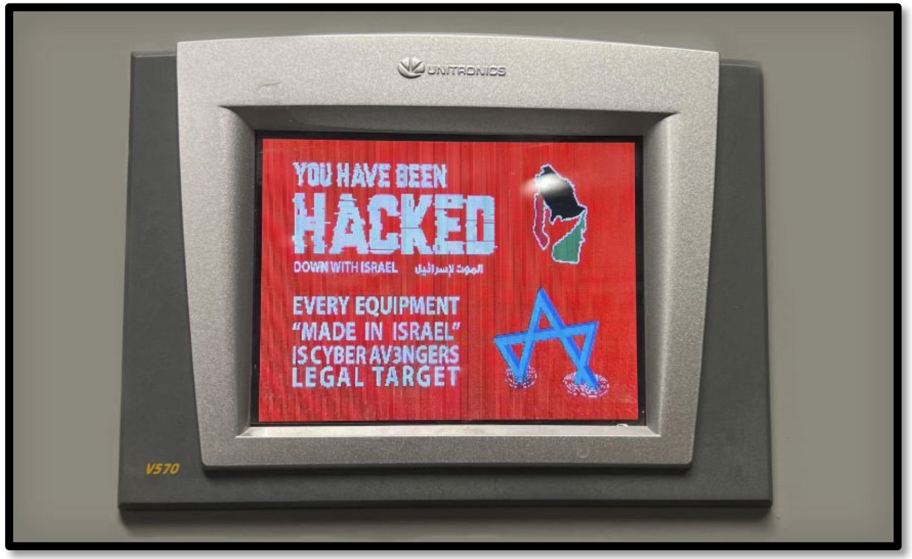
Pro-Russia hacktivist activity against these sectors appears mostly limited to unsophisticated techniques that manipulate ICS equipment to create nuisance effects. However, investigations have identified that these actors are capable of techniques that pose physical threats against *insecure and misconfigured* OT environments. Pro-Russia hacktivists have been observed gaining remote access via a combination of exploiting publicly exposed internet-facing connections and outdated VNC software, as well as using the HMIs' factory default passwords and weak passwords without multifactor authentication.

TLP:CLEAR

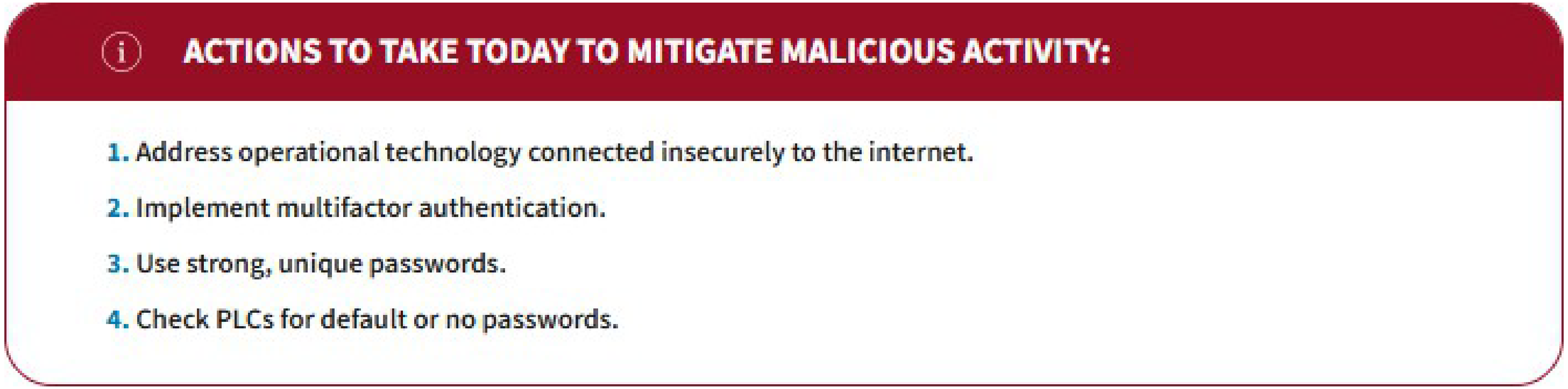
cisa.gov central@cisa.dhs.gov @CISAgov | @CISACyber @cisagov As of May 1, 2024

Iranian Threat Actor: CyberAv3ngers

- In November 2023, the CyberAv3ngers began targeting and compromising Israeli-made programmable logic controllers (PLCs) and human machine interfaces (HMIs).
- Impacted multiple sectors, including U.S. water and wastewater systems, and resulted in operational impacts.



CARR & Cyber Av3ngers: Mitigation Actions



ⓘ **ACTIONS TO TAKE TODAY TO MITIGATE MALICIOUS ACTIVITY:**

1. Address operational technology connected insecurely to the internet.
2. Implement multifactor authentication.
3. Use strong, unique passwords.
4. Check PLCs for default or no passwords.

PRC Threat Actor: Volt Typhoon

- People's Republic of China (PRC) state-sponsored actor that has been actively targeting critical infrastructure in the United States, including water and wastewater systems.
- Conducts extensive pre-compromise reconnaissance and gain initial access to IT networks by exploiting public-facing assets.

JOINT CYBERSECURITY ADVISORY

Co-Authored by:

TLP:CLEAR

Product ID: AA24-038A

February 7, 2024

Australian Government
Australian Signals Directorate

ASD Australian Signals Directorate
ACSC

Communications Security Establishment
Canadian Centre for Cyber Security

Centre de la sécurité des télécommunications
Centre canadien pour la cybersécurité

National Cyber Security Centre
PART OF THE GCSB

National Cyber Security Centre
a part of GCHQ

PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure

PRC Threat Actor: Volt Typhoon

- After gaining access to a victim's network, the group uses “Living Off the Land" techniques to evade detection.
- Use elevated credentials for additional discovery, often focusing on gaining capabilities to access OT assets.

JOINT CYBERSECURITY ADVISORY

Co-Authored by:

TLP:CLEAR

Product ID: AA24-038A

February 7, 2024

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC

Communications Security Establishment
Canadian Centre for Cyber Security

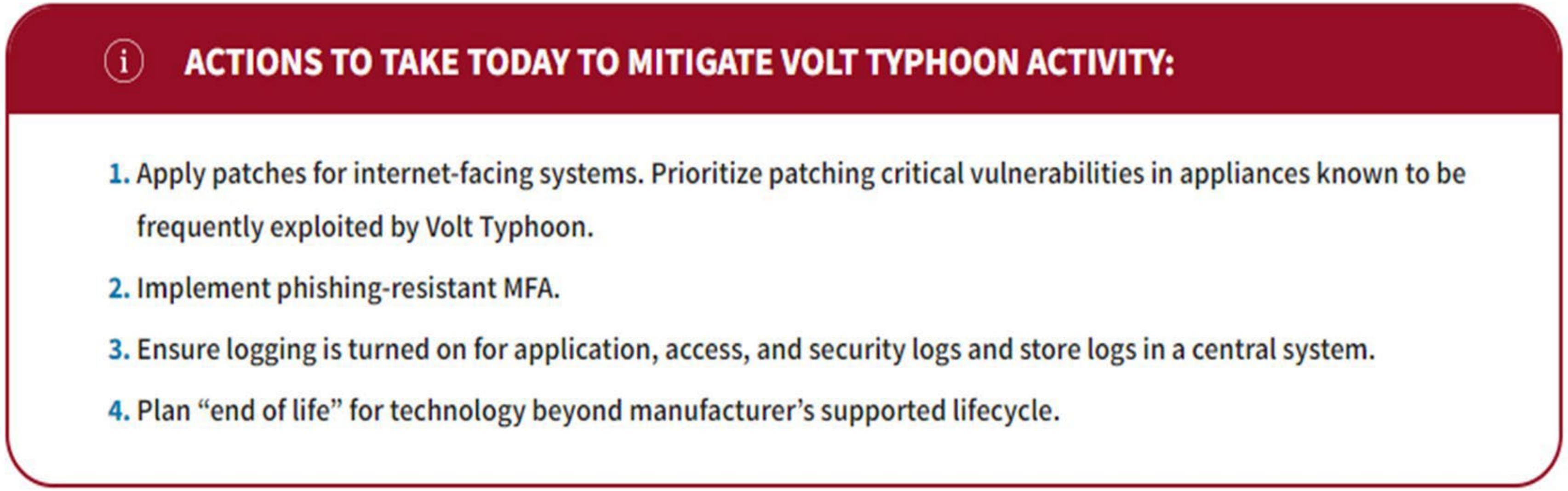
Centre de la sécurité des télécommunications
Centre canadien pour la cybersécurité

National Cyber Security Centre
PART OF THE GCSB

National Cyber Security Centre
a part of GCHQ

PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure

Volt Typhoon: Mitigation Actions



ACTIONS TO TAKE TODAY TO MITIGATE VOLT TYPHOON ACTIVITY:

1. Apply patches for internet-facing systems. Prioritize patching critical vulnerabilities in appliances known to be frequently exploited by Volt Typhoon.
2. Implement phishing-resistant MFA.
3. Ensure logging is turned on for application, access, and security logs and store logs in a central system.
4. Plan “end of life” for technology beyond manufacturer’s supported lifecycle.

Targeting of ICS/SCADA Devices

ICS/SCADA Overview

- Industrial Control Systems (ICS)
  - A collection of control systems and other hardware that work together to automate or operate industrial processes.
  - The goal of ICSs is to make daily operations more efficient and autonomous, with minimal human input.
- Supervisory Control and Data Acquisition (SCADA)
  - A computerized system that uses software and hardware to monitor and control industrial processes and equipment.
  - Allows operator to supervise the equipment and control them remotely
  - Examines, collects and processes data in real-time.

What is an Insider Threat?

- The potential for an insider to use their authorized access or understanding of an organization to harm that organization.
- Examples:
  - Shadow IT
  - Terrorism
  - Unauthorized disclosure of information
  - Corruption
  - Sabotage
  - Workplace violence
  - Intentional or unintentional loss or degradation of resources or capabilities

Preventing Insider Threats

- Security Policy
  - Define security controls to identify and prevent malicious behaviors and block unauthorized users.
- Revoke Access
  - Remove/Disable account of users who have retired, changed roles, or separated from the organization.
- Cyber Awareness Training
  - Accidents happen, but training users on what to watch out for minimizes those accidents.
- Strong Authentication
  - Enhancing authentication methods reduces the risk of unauthorized access.

What is Social Engineering?

- Social engineering is manipulating people so they give up confidential information.
- How is it done?
  - Phishing emails (Friends or Trusted Sources)
  - Spear Phishing (Targeted form of phishing)
  - Whaling (Targets high-level executive)
  - Smishing (SMS message based)
  - Tailgating/Piggybacking (enter behind someone or get them to hold door)

Preventing Social Engineering

- Do:
  - Check validity of sources
  - Remain vigilant of surroundings
  - Enable Multifactor Authentication (MFA)
  - Regularly update and patch systems

- Don’t:
  - Respond to urgent requests
  - Share personal information
  - Insert unknown USB or other devices
  - Click a link or download files from an unfamiliar or suspicious sender

What is Malware?

- Malware is any software that is intentionally designed to harm or exploit a computer, network, or server
  - General term
- A virus is a type of malware that can attach itself to other programs, replicate and spread to other devices
  - Specific term

How Malware Spreads

- Email
  - Fake FedEx email stating you missed a package and must click a link to set a new delivery date.
- Websites
  - Pop-up ad telling you that you have a virus you need to remove immediately.
- Phone
  - Fake call from your IT department that requested permission to remotely access your computer.
- Apps
  - Malicious code in a popular app advertising a free app for downloading.

Preventing Malware

- Regular Software Updates
  - Newer versions often contain more security fixes to prevent malware attacks.
- Anti-Malware Software
  - Install and update anti-malware or anti-virus software and set it to update automatically.
  - Use a firewall.
- Safe Browsing Practices
  - Be cautious of websites, downloads and emails.
- Portable Storage Device Hygiene
  - Test or inspect portable storage devices (e.g., USB/flash drives) prior to connecting them to a network.

Malware

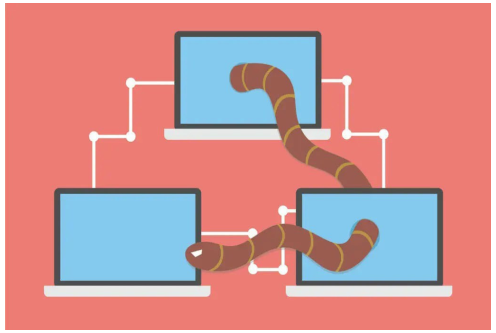
Types of Malware

Adware

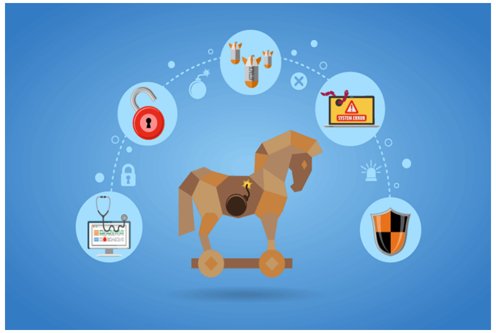
Ransomware

Spyware

Worm



Trojan



Poll 2

Types of Malware: Adware

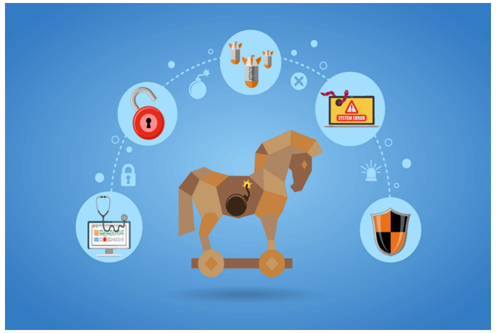
- Secretly installs itself on your device and displays unwanted advertisements and pop-ups.
- Disguises itself as legitimate, or piggybacks on another program to trick you into installing it on your PC, tablet or mobile device.
- Can track you online to provide personalized ads.

Types of Malware: Ransomware

- Prevents users from accessing their system or personal files and demands ransom payment to regain access.
- Comes from social engineering or “tricking users.”
- Ransom payments are demanded as cryptocurrency or credit card payments.

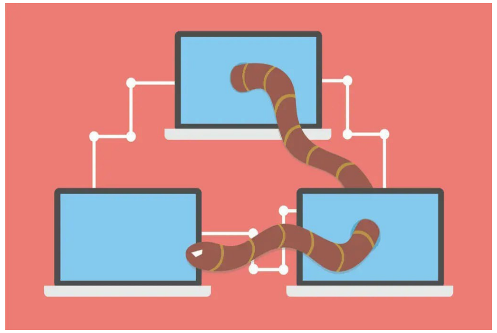
Types of Malware: Trojans

- “A Trojan can be a Swiss Army knife of hacking.”
- Various types of Trojan objectives:
    - Standalone malware
    - Delivering payloads
    - Communicating back with the hacker
    - Opening the system (from the inside) to further attacks



Types of Malware: Worm

- Capable of propagating or replicating itself from one system to another.
- Can do malicious tasks:
  - Dropping other malware
  - Copying itself onto devices physically attached (USBs, Storage Devices)
  - Deleting files
  - Consuming bandwidth



Types of Malware: Spyware

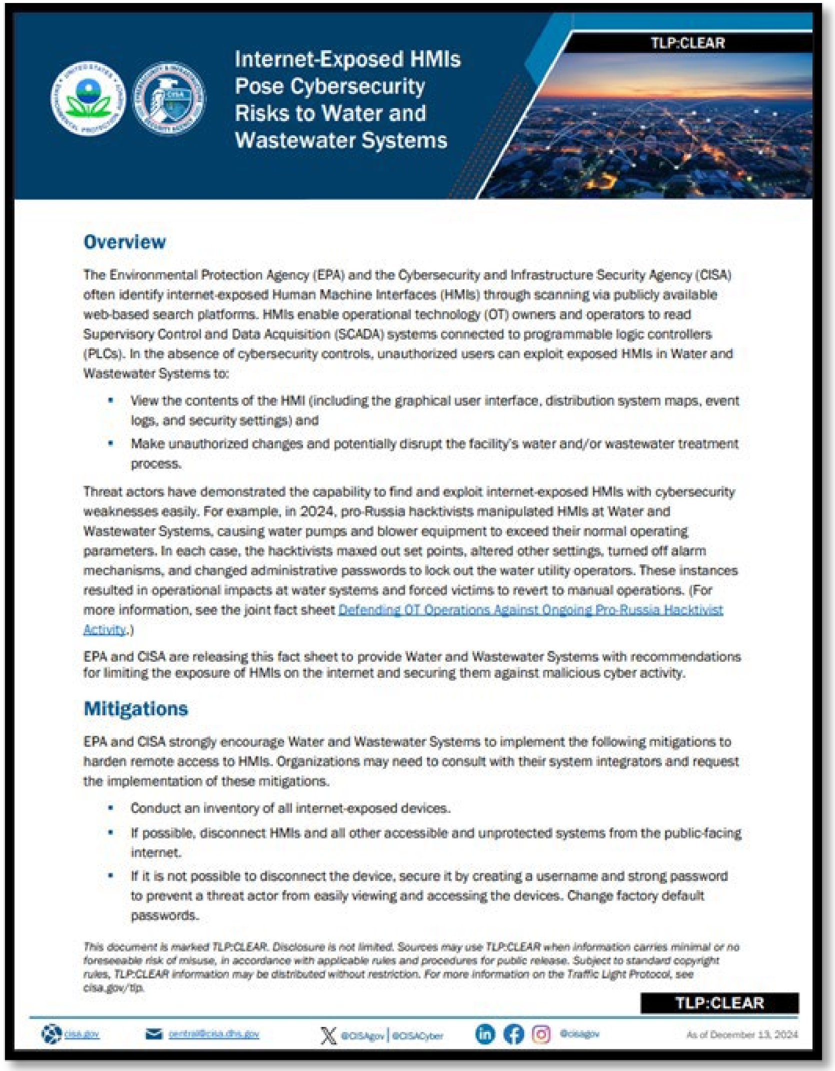
- Invades the device, steals sensitive information and internet usage data, and relays it to advertisers, data firms or external users.
- Once Installed:
  - Monitors Internet activity
  - Tracks login credentials
  - Spies on sensitive information
- Primary Goal: Obtain credit card numbers, banking information and passwords.

BREAK

Human-Machine Interface Threats

Internet-Exposed HMIs Pose Cybersecurity Risks to Water and Wastewater Systems

- EPA and CISA often identify internet-exposed Human Machine Interfaces (HMIs) through scanning via publicly available web-based search platforms.
- In the absence of cybersecurity controls, unauthorized users can exploit HMIs to:
  - View the contents of the HMI
  - Make unauthorized changes and potentially disrupt the facility's water and/or wastewater treatment process



TLP:CLEAR

Internet-Exposed HMIs Pose Cybersecurity Risks to Water and Wastewater Systems

Overview

The Environmental Protection Agency (EPA) and the Cybersecurity and Infrastructure Security Agency (CISA) often identify internet-exposed Human Machine Interfaces (HMIs) through scanning via publicly available web-based search platforms. HMIs enable operational technology (OT) owners and operators to read Supervisory Control and Data Acquisition (SCADA) systems connected to programmable logic controllers (PLCs). In the absence of cybersecurity controls, unauthorized users can exploit exposed HMIs in Water and Wastewater Systems to:

- View the contents of the HMI (including the graphical user interface, distribution system maps, event logs, and security settings) and
- Make unauthorized changes and potentially disrupt the facility's water and/or wastewater treatment process.

Threat actors have demonstrated the capability to find and exploit internet-exposed HMIs with cybersecurity weaknesses easily. For example, in 2024, pro-Russia hacktivists manipulated HMIs at Water and Wastewater Systems, causing water pumps and blower equipment to exceed their normal operating parameters. In each case, the hacktivists maxed out set points, altered other settings, turned off alarm mechanisms, and changed administrative passwords to lock out the water utility operators. These instances resulted in operational impacts at water systems and forced victims to revert to manual operations. (For more information, see the joint fact sheet Defending OT Operations Against Ongoing Pro-Russia Hacktivist Activity.)

EPA and CISA are releasing this fact sheet to provide Water and Wastewater Systems with recommendations for limiting the exposure of HMIs on the internet and securing them against malicious cyber activity.

Mitigations

EPA and CISA strongly encourage Water and Wastewater Systems to implement the following mitigations to harden remote access to HMIs. Organizations may need to consult with their system integrators and request the implementation of these mitigations.

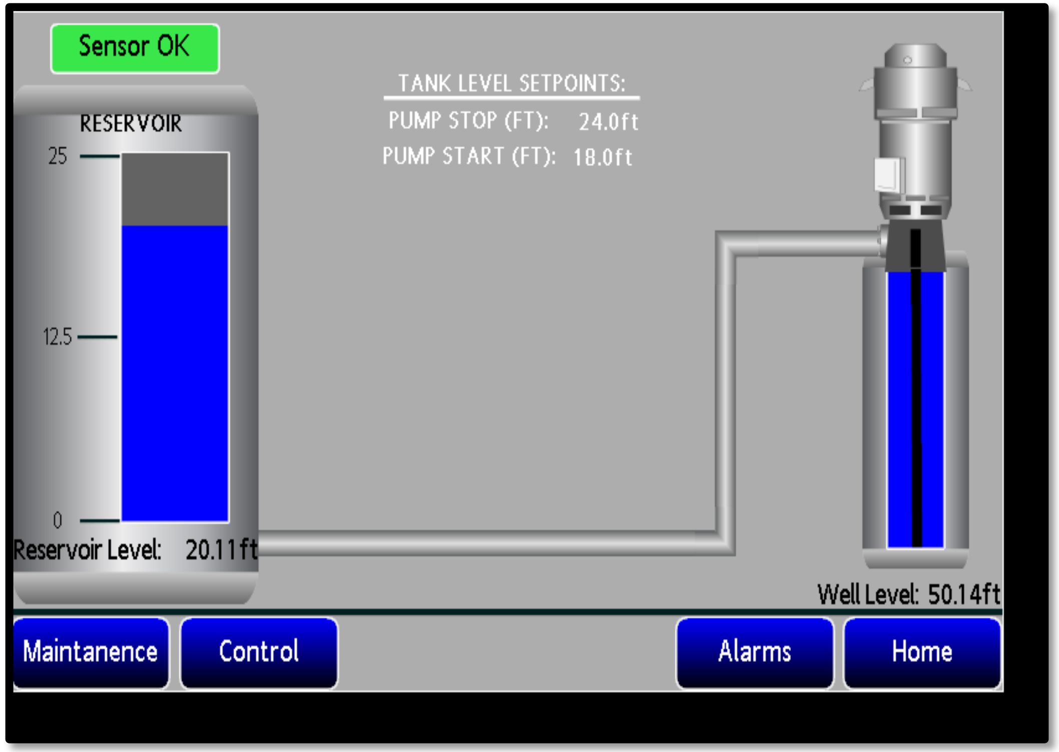
- Conduct an inventory of all internet-exposed devices.
- If possible, disconnect HMIs and all other accessible and unprotected systems from the public-facing internet.
- If it is not possible to disconnect the device, secure it by creating a username and strong password to prevent a threat actor from easily viewing and accessing the devices. Change factory default passwords.

This document is marked TLP:CLEAR. Disclosure is not limited. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be distributed without restriction. For more information on the Traffic Light Protocol, see cisa.gov/tlp.

TLP:CLEAR

cisa.gov central@cisa.dhs.gov @CISAgov | @CISACyber @cisagov As of December 13, 2024

Example of Exposed HMIs



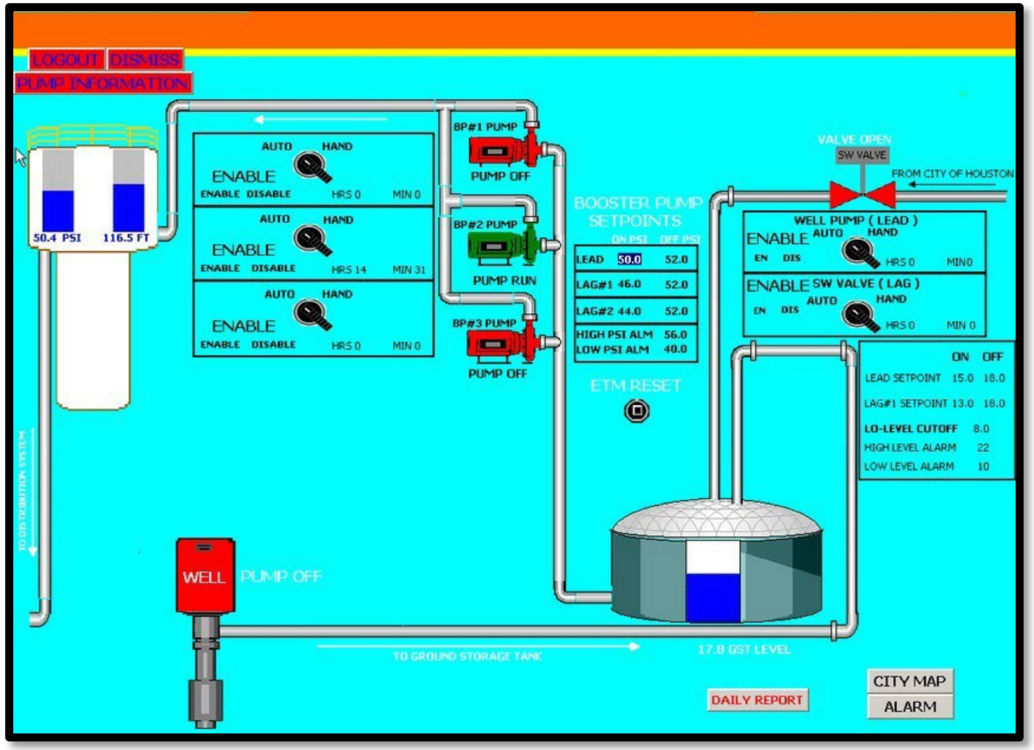
TANK LEVEL SETPOINTS:

PUMP STOP (FT): 24.0ft

PUMP START (FT): 18.0ft

Reservoir Level: 20.11ft

Well Level: 50.14ft



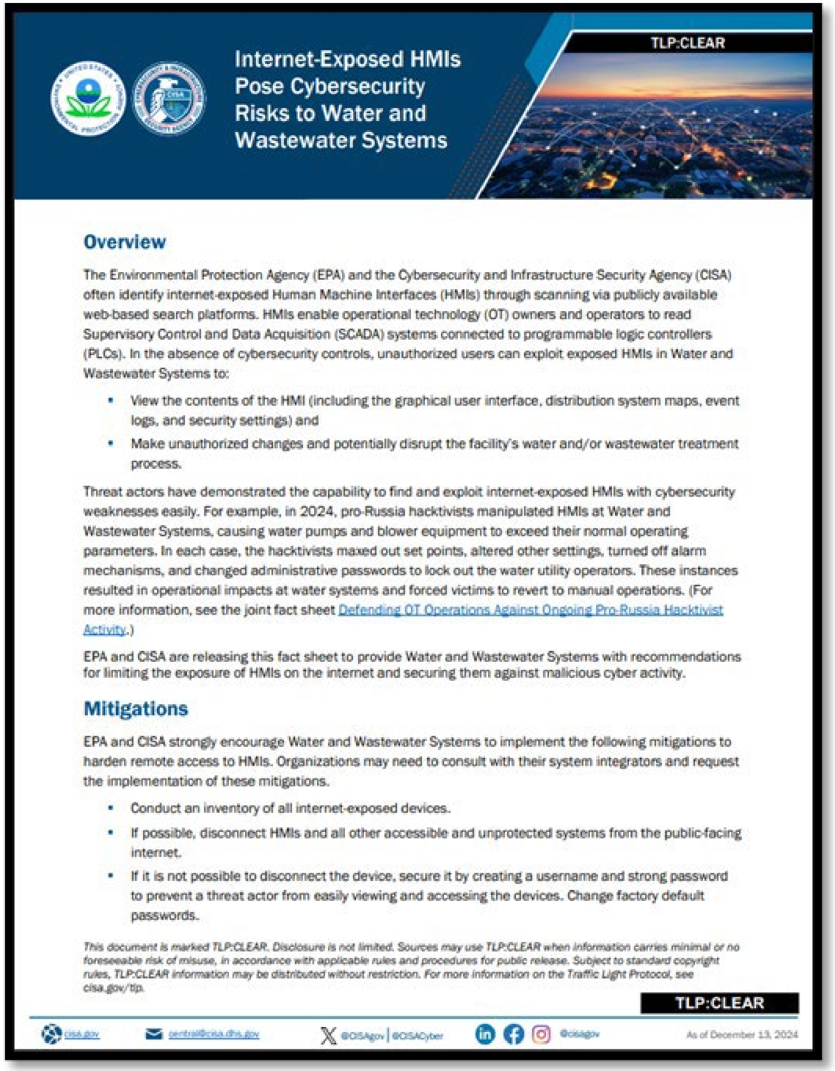
BOOSTER PUMP SETPOINTS

	ON PSI	OFF PSI
LEAD	50.0	52.0
LAG#1	46.0	52.0
LAG#2	44.0	52.0
HIGH PSI ALM	56.0	
LOW PSI ALM	40.0	

	ON	OFF
LEAD SETPOINT	15.0	18.0
LAG#1 SETPOINT	13.0	18.0
LO-LEVEL CUTOFF	8.0	
HIGH LEVEL ALARM	22	
LOW LEVEL ALARM	10	

Internet-Exposed HMIs Mitigation

1. Conduct an inventory of all internet-exposed devices.
2. If possible, disconnect HMIs from the public internet. If this is not possible, secure HMIs with strong passwords and never use factory default passwords.
3. Log remote logins to HMIs.
4. Implement vendor security recommendations.
5. Keep all systems up to date with patches and security updates.
6. Implement Multi-Factor Authentication (MFA) for all access to HMIs and the OT network.
7. Implement network segmentation.



TLP:CLEAR

Internet-Exposed HMIs Pose Cybersecurity Risks to Water and Wastewater Systems

Overview

The Environmental Protection Agency (EPA) and the Cybersecurity and Infrastructure Security Agency (CISA) often identify internet-exposed Human Machine Interfaces (HMIs) through scanning via publicly available web-based search platforms. HMIs enable operational technology (OT) owners and operators to read Supervisory Control and Data Acquisition (SCADA) systems connected to programmable logic controllers (PLCs). In the absence of cybersecurity controls, unauthorized users can exploit exposed HMIs in Water and Wastewater Systems to:

- View the contents of the HMI (including the graphical user interface, distribution system maps, event logs, and security settings) and
- Make unauthorized changes and potentially disrupt the facility's water and/or wastewater treatment process.

Threat actors have demonstrated the capability to find and exploit internet-exposed HMIs with cybersecurity weaknesses easily. For example, in 2024, pro-Russia hacktivists manipulated HMIs at Water and Wastewater Systems, causing water pumps and blower equipment to exceed their normal operating parameters. In each case, the hacktivists maxed out set points, altered other settings, turned off alarm mechanisms, and changed administrative passwords to lock out the water utility operators. These instances resulted in operational impacts at water systems and forced victims to revert to manual operations. (For more information, see the joint fact sheet Defending OT Operations Against Ongoing Pro-Russia Hacktivist Activity.)

EPA and CISA are releasing this fact sheet to provide Water and Wastewater Systems with recommendations for limiting the exposure of HMIs on the internet and securing them against malicious cyber activity.

Mitigations

EPA and CISA strongly encourage Water and Wastewater Systems to implement the following mitigations to harden remote access to HMIs. Organizations may need to consult with their system integrators and request the implementation of these mitigations.

- Conduct an inventory of all internet-exposed devices.
- If possible, disconnect HMIs and all other accessible and unprotected systems from the public-facing internet.
- If it is not possible to disconnect the device, secure it by creating a username and strong password to prevent a threat actor from easily viewing and accessing the devices. Change factory default passwords.

This document is marked TLP:CLEAR. Disclosure is not limited. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be distributed without restriction. For more information on the Traffic Light Protocol, see cisa.gov/tlp.

TLP:CLEAR

cisa.gov central@cisa.dhs.gov @CISAgov | @CISACyber @cisagov As of December 13, 2024

Other Examples of Cybersecurity Threats & Incidents at Water Systems

EPA Water Infrastructure & Cyber Resilience Division

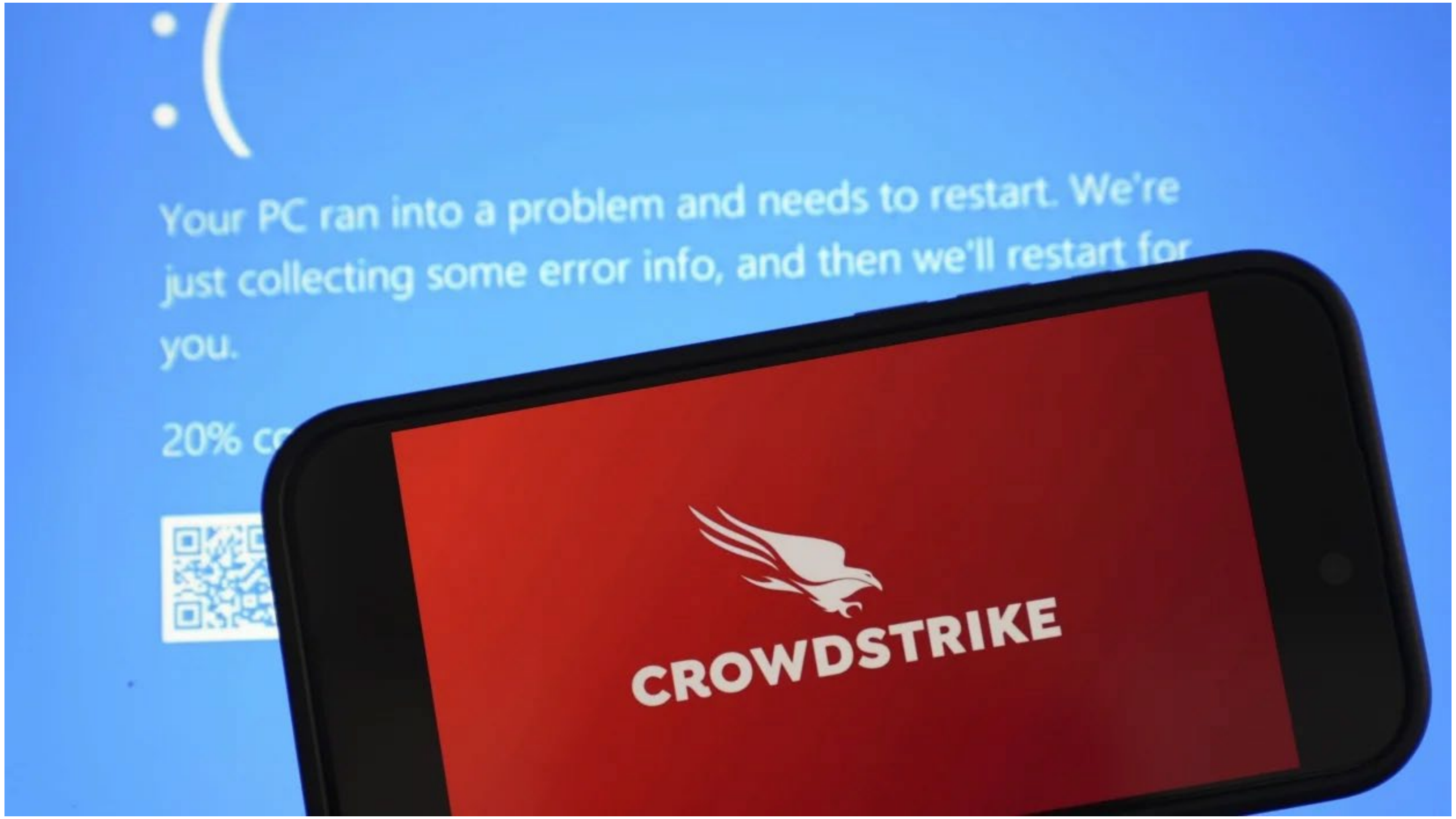
Ongoing Cyber Threats to U.S. Water & Wastewater Systems

- October 2024 | American Water – one of the nation’s largest water utilities that supplies water to more than 14 million people – discovered that it was the victim of a cybersecurity incident that breached its networks and systems, including its customer billing system. The utility disconnected or deactivated certain systems to protect customer data. Operations were not impacted by the breach.
- July 2023 | Discovery Bay, CA | Previous contracted employee posed an insider threat when he hacked into the water treatment facility's computer network, uninstalling software that regulated water pressure, filtration, and chemical levels.
- May 2023 | U.S. Military Installations | Chinese government-backed hacker group has inserted malware into systems of numerous water and electric utilities that serve U.S. military installations.

Ongoing Cyber Threats to U.S. Water & Wastewater Systems

- March 2019 | Ellsworth County, KS | Former employee acted as insider threat by using their credentials, which had not yet been revoked, to remotely access the facility's information systems and attempted to alter treatment of drinking water.
- October 2018 | Jacksonville, NC | Emotet ransomware was reported to have spread through Onslow Water and Sewer Authority's information systems, followed by Ryuk ransomware ten days later. The IT infrastructure had to be shut down to limit spread of malware.
- April 2016 | Lansing, MI | A utility chose to pay a $25,000 ransom to resume business operations after they fell victim to a ransomware attack through a malicious email attachment clicked by an employee.

CrowdStrike


:(
Your PC ran into a problem and needs to restart. We're just collecting some error info, and then we'll restart for you.
20% co
CROWDSTRIKE

CrowdStrike

- An update containing “incorrect code” affected systems running Windows 10 or later
  - Caused systems to crash, leading to multiple services unavailable

- Impacted utility SCADA systems and various utility computers taking them offline
  - Utilities were able to address issue in a timely manner and maintain operations

Stay Informed

Register for EPA’s Water Sector Alerts

DHS Office of Intelligence and Analysis (I&A)

- DHS I&A's Cyber Intelligence Center (CIC) hosts an UNCLASSIFIED//FOR OFFICIAL USE ONLY Bi-weekly Cyber Threat Intelligence Teleconference.
- The teleconference highlights current and emerging issues in the cyber threat landscape.
- Recommended participants include public and private sector cybersecurity and/or intelligence professionals who support cybersecurity or critical infrastructure security.
- If you are interested in attending this call, contact cyber@hq.dhs.gov.

CISA Resources

- Known Exploited Vulnerabilities(KEV) Catalog
  - A list of currently known vulnerabilities
  - https://www.cisa.gov/known-exploited-vulnerabilities-catalog

- Cyber Alerts
  - Receive vital information on new threats
  - https://public.govdelivery.com/accounts/USDHSCISA/subscriber/new?qsp=CODE_RED

Cybersecurity Incident Reporting

EPA | Water Infrastructure & Cyber Resilience Division

Cybersecurity Incident Reporting

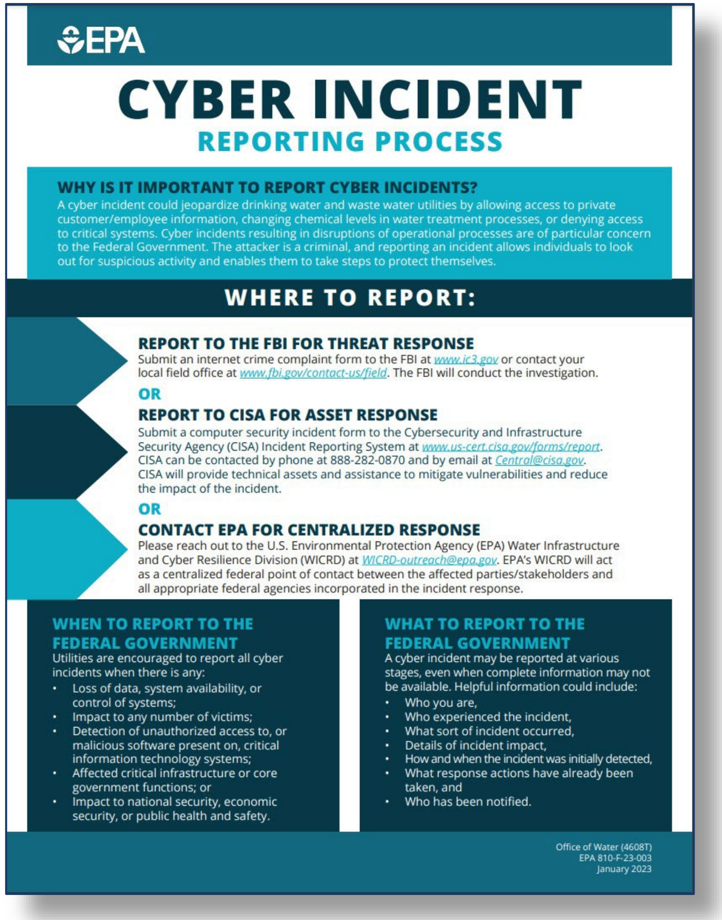
Why is incident reporting important?

- Allows rapid deployment of resources to assist victims.
- Facilitates analysis of incoming reporting across sectors to spot trends.
- Expedites information sharing to warn other potential victims.
- Promotes information sharing on tactics, techniques, and procedures.

Poll 3

EPA Cybersecurity Incident Reporting Fact Sheet

- The Fact Sheet features:
  - Importance of reporting
  - Where to report
    - FBI (ic3.gov)
    - CISA
    - EPA
  - When to report
  - What to report



EPA

CYBER INCIDENT
REPORTING PROCESS

WHY IS IT IMPORTANT TO REPORT CYBER INCIDENTS?
A cyber incident could jeopardize drinking water and waste water utilities by allowing access to private customer/employee information, changing chemical levels in water treatment processes, or denying access to critical systems. Cyber incidents resulting in disruptions of operational processes are of particular concern to the Federal Government. The attacker is a criminal, and reporting an incident allows individuals to look out for suspicious activity and enables them to take steps to protect themselves.

WHERE TO REPORT:

REPORT TO THE FBI FOR THREAT RESPONSE
Submit an internet crime complaint form to the FBI at *www.ic3.gov* or contact your local field office at *www.fbi.gov/contact-us/field*. The FBI will conduct the investigation.

OR

REPORT TO CISA FOR ASSET RESPONSE
Submit a computer security incident form to the Cybersecurity and Infrastructure Security Agency (CISA) Incident Reporting System at *www.us-cert.cisa.gov/forms/report*. CISA can be contacted by phone at 888-282-0870 and by email at *Central@cisa.gov*. CISA will provide technical assets and assistance to mitigate vulnerabilities and reduce the impact of the incident.

OR

CONTACT EPA FOR CENTRALIZED RESPONSE
Please reach out to the U.S. Environmental Protection Agency (EPA) Water Infrastructure and Cyber Resilience Division (WICRD) at *WICRD-outreach@epa.gov*. EPA's WICRD will act as a centralized federal point of contact between the affected parties/stakeholders and all appropriate federal agencies incorporated in the incident response.

WHEN TO REPORT TO THE FEDERAL GOVERNMENT
Utilities are encouraged to report all cyber incidents when there is any:
- Loss of data, system availability, or control of systems;
- Impact to any number of victims;
- Detection of unauthorized access to, or malicious software present on, critical information technology systems;
- Affected critical infrastructure or core government functions; or
- Impact to national security, economic security, or public health and safety.

WHAT TO REPORT TO THE FEDERAL GOVERNMENT
A cyber incident may be reported at various stages, even when complete information may not be available. Helpful information could include:
- Who you are,
- Who experienced the incident,
- What sort of incident occurred,
- Details of incident impact,
- How and when the incident was initially detected,
- What response actions have already been taken, and
- Who has been notified.

Office of Water (4608T)
EPA 810-F-23-003
January 2023

https://www.epa.gov/system/files/documents/2023-02/230202-CyberIncidentReportingProcess_21118.pdf

Cybersecurity Courses for the Water Sector

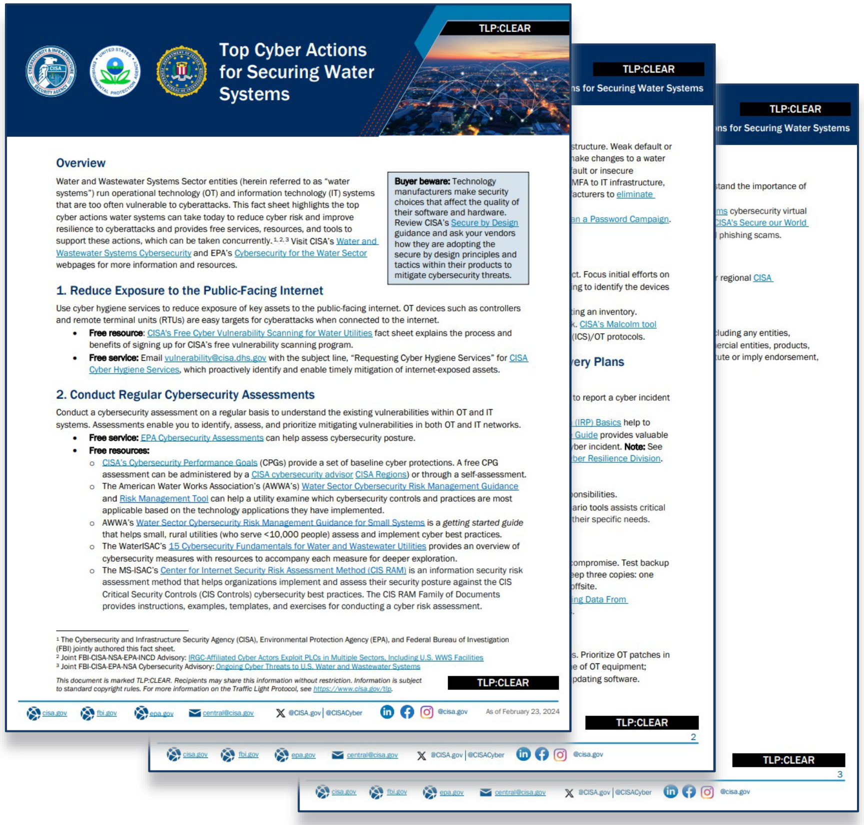
- EPA is committed to providing cybersecurity courses for the water sector on an ongoing and reoccurring basis.
- Courses include cybersecurity basics for water systems, how to conduct a cybersecurity risk assessment, tabletop exercises, and more.
- Visit www.epa.gov/waterresilience/cybersecurity-exercises-and-technical-assistance-courses to view upcoming and recorded exercises.
- Contact watercyberta@epa.gov to request a cybersecurity technical assistance course or tabletop exercise.

EPA Cybersecurity Resources

EPA | Water Infrastructure &
Cyber Resilience Division

Top Cyber Actions for Securing Water Systems OT

1. Reduce exposure to the public-facing internet
2. Conduct regular cybersecurity assessments
3. Change default passwords
4. Conduct and inventory of OT/IT assets
5. Develop and exercise cybersecurity incident response and recovery plans
6. Backup OT/IT systems
7. Reduce exposure to vulnerabilities
8. Conduct cybersecurity awareness training



TLP:CLEAR

Top Cyber Actions for Securing Water Systems

Overview

Water and Wastewater Systems Sector entities (herein referred to as "water systems") run operational technology (OT) and information technology (IT) systems that are too often vulnerable to cyberattacks. This fact sheet highlights the top cyber actions water systems can take today to reduce cyber risk and improve resilience to cyberattacks and provides free services, resources, and tools to support these actions, which can be taken concurrently.[1, 2, 3] Visit CISA's Water and Wastewater Systems Cybersecurity and EPA's Cybersecurity for the Water Sector webpages for more information and resources.

Buyer beware: Technology manufacturers make security choices that affect the quality of their software and hardware. Review CISA's Secure by Design guidance and ask your vendors how they are adopting the secure by design principles and tactics within their products to mitigate cybersecurity threats.

1. Reduce Exposure to the Public-Facing Internet

Use cyber hygiene services to reduce exposure of key assets to the public-facing internet. OT devices such as controllers and remote terminal units (RTUs) are easy targets for cyberattacks when connected to the 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

Conduct a cybersecurity assessment on a regular basis to understand the existing vulnerabilities within OT and IT systems. Assessments enable you to identify, assess, and prioritize mitigating vulnerabilities in both OT and IT networks.

- **Free service:** EPA Cybersecurity Assessments can help assess cybersecurity posture.
- **Free resources:**
  - CISA's Cybersecurity Performance Goals (CPGs) provide a set of baseline cyber protections. A free CPG assessment can be administered by a CISA cybersecurity advisor CISA Regions) or through a self-assessment.
  - The American Water Works Association's (AWWA's) Water Sector Cybersecurity Risk Management Guidance and Risk Management Tool can help a utility examine which cybersecurity controls and practices are most applicable based on the technology applications they have implemented.
  - AWWA's Water Sector Cybersecurity Risk Management Guidance for Small Systems is a *getting started guide* that helps small, rural utilities (who serve <10,000 people) assess and implement cyber best practices.
  - The WaterISAC's 15 Cybersecurity Fundamentals for Water and Wastewater Utilities provides an overview of cybersecurity measures with resources to accompany each measure for deeper exploration.
  - The MS-ISAC's Center for Internet Security Risk Assessment Method (CIS RAM) is an information security risk assessment method that helps organizations implement and assess their security posture against the CIS Critical Security Controls (CIS Controls) cybersecurity best practices. The CIS RAM Family of Documents provides instructions, examples, templates, and exercises for conducting a cyber risk assessment.

[1] The Cybersecurity and Infrastructure Security Agency (CISA), Environmental Protection Agency (EPA), and Federal Bureau of Investigation (FBI) jointly authored this fact sheet.
[2] Joint FBI-CISA-NSA-EPA-INCD Advisory: IRGC-Affiliated Cyber Actors Exploit PLCs in Multiple Sectors, Including U.S. WWS Facilities
[3] Joint FBI-CISA-EPA-NSA Cybersecurity Advisory: Ongoing Cyber Threats to U.S. Water and Wastewater Systems

This document is marked TLP:CLEAR. Recipients may share this information without restriction. Information is subject to standard copyright rules. For more information on the Traffic Light Protocol, see https://www.cisa.gov/tlp.

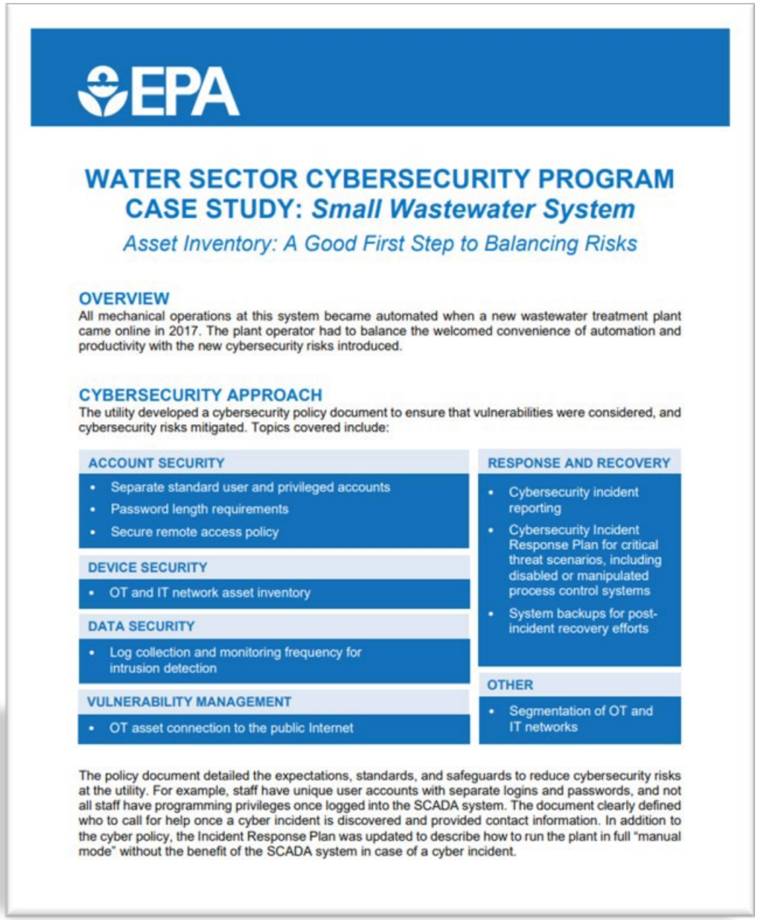
TLP:CLEAR

cisa.gov fbi.gov epa.gov central@cisa.gov @CISA.gov | @CISACyber @cisa.gov As of February 23, 2024

Poll 4

EPA’s Water Sector Cybersecurity Program Case Studies

- Case studies highlighting the cybersecurity success stories at water and wastewater utilities.
  - Small Combined System
  - Small Wastewater System
  - Medium Drinking Water System
  - Medium Drinking Water System #2
  - Medium Combined System
  - Large Combined System



EPA

WATER SECTOR CYBERSECURITY PROGRAM
CASE STUDY: *Small Wastewater System*

Asset Inventory: A Good First Step to Balancing Risks

OVERVIEW

All mechanical operations at this system became automated when a new wastewater treatment plant came online in 2017. The plant operator had to balance the welcomed convenience of automation and productivity with the new cybersecurity risks introduced.

CYBERSECURITY APPROACH

The utility developed a cybersecurity policy document to ensure that vulnerabilities were considered, and cybersecurity risks mitigated. Topics covered include:

ACCOUNT SECURITY
- Separate standard user and privileged accounts
- Password length requirements
- Secure remote access policy

DEVICE SECURITY
- OT and IT network asset inventory

DATA SECURITY
- Log collection and monitoring frequency for intrusion detection

VULNERABILITY MANAGEMENT
- OT asset connection to the public Internet

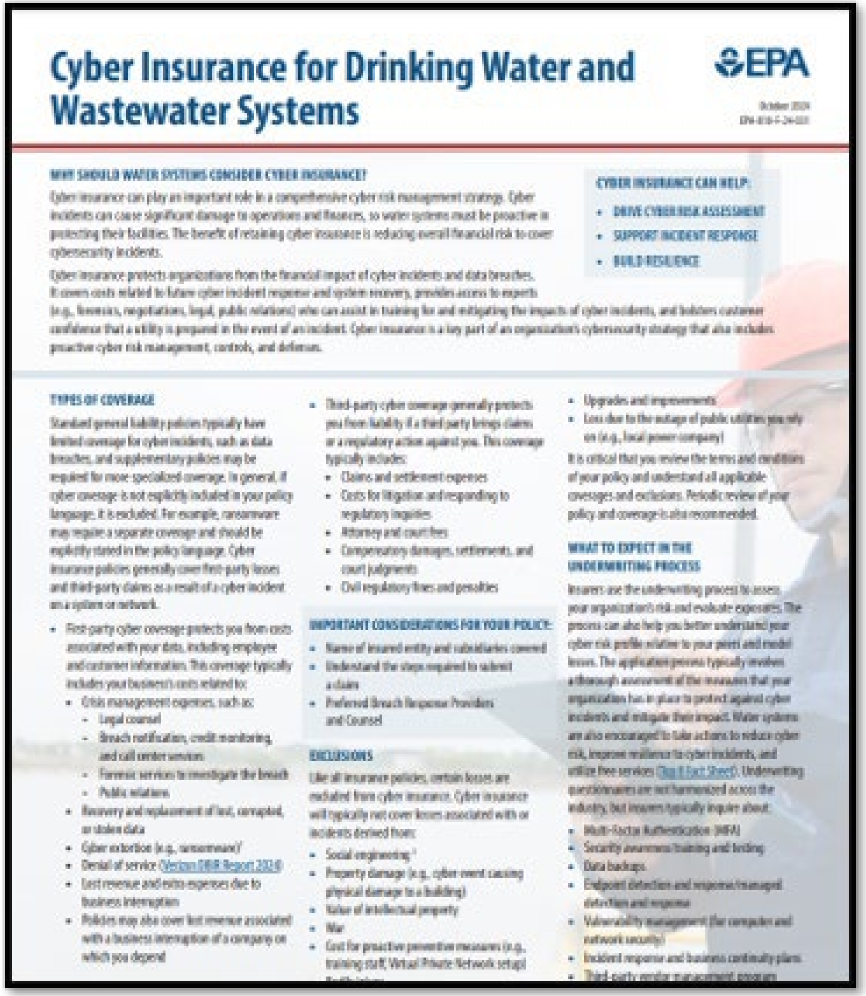
RESPONSE AND RECOVERY
- Cybersecurity incident reporting
- Cybersecurity Incident Response Plan for critical threat scenarios, including disabled or manipulated process control systems
- System backups for post-incident recovery efforts

OTHER
- Segmentation of OT and IT networks

The policy document detailed the expectations, standards, and safeguards to reduce cybersecurity risks at the utility. For example, staff have unique user accounts with separate logins and passwords, and not all staff have programming privileges once logged into the SCADA system. The document clearly defined who to call for help once a cyber incident is discovered and provided contact information. In addition to the cyber policy, the Incident Response Plan was updated to describe how to run the plant in full “manual mode” without the benefit of the SCADA system in case of a cyber incident.

Fact Sheet: Cyber Insurance for Drinking Water and Wastewater Systems

- Provides an in-depth overview of cybersecurity insurance for water and wastewater systems.
- Demonstrates the important role cyber insurance plays in a comprehensive cyber risk management strategy.



Cyber Insurance for Drinking Water and Wastewater Systems

EPA

October 2024
EPA-816-F-24-[illegible]

WHY SHOULD WATER SYSTEMS CONSIDER CYBER INSURANCE?

Cyber insurance can play an important role in a comprehensive cyber risk management strategy. Cyber incidents can cause significant damage to operations and finances, so water systems must be proactive in protecting their facilities. The benefit of retaining cyber insurance is reducing overall financial risk to cover cybersecurity incidents.

Cyber insurance protects organizations from the financial impact of cyber incidents and data breaches. It covers costs related to future cyber incident response and system recovery, provides access to experts (e.g., forensics, negotiations, legal, public relations) who can assist in training for and mitigating the impacts of cyber incidents, and bolsters customer confidence that a utility is prepared in the event of an incident. Cyber insurance is a key part of an organization's cybersecurity strategy that also includes proactive cyber risk management, controls, and defenses.

CYBER INSURANCE CAN HELP:

- DRIVE CYBER RISK ASSESSMENT
- SUPPORT INCIDENT RESPONSE
- BUILD RESILIENCE

TYPES OF COVERAGE

Standard general liability policies typically have limited coverage for cyber incidents, such as data breaches, and supplementary policies may be required for more specialized coverage. In general, if cyber coverage is not explicitly included in your policy language, it is excluded. For example, ransomware may require a separate coverage and should be explicitly stated in the policy language. Cyber insurance policies generally cover first-party losses and third-party claims as a result of a cyber incident on a system or network.

- First-party cyber coverage protects you from costs associated with your data, including employee and customer information. This coverage typically includes your business's costs related to:
  - Crisis management expenses, such as:
    - Legal counsel
    - Breach notification, credit monitoring, and call center services
    - Forensic services to investigate the breach
    - Public relations
  - Recovery and replacement of lost, corrupted, or stolen data
  - Cyber extortion (e.g., ransomware)
  - Denial of service (Verizon DBIR Report 2024)
  - Lost revenue and extra expenses due to business interruption
  - Policies may also cover lost revenue associated with a business interruption of a company on which you depend
- Third-party cyber coverage generally protects you from liability if a third party brings claims or a regulatory action against you. This coverage typically includes:
  - Claims and settlement expenses
  - Costs for litigation and responding to regulatory inquiries
  - Attorney and court fees
  - Compensatory damages, settlements, and court judgments
  - Civil regulatory fines and penalties

IMPORTANT CONSIDERATIONS FOR YOUR POLICY:

- Name of insured entity and subsidiaries covered
- Understand the steps required to submit a claim
- Preferred Breach Response Providers and Counsel

EXCLUSIONS

Like all insurance policies, certain losses are excluded from cyber insurance. Cyber insurance will typically not cover losses associated with or incidents derived from:

- Social engineering[1]
- Property damage (e.g., cyber event causing physical damage to a building)
- Value of intellectual property
- War
- Cost for proactive preventive measures (e.g., training staff, Virtual Private Network setup)
- Upgrades and improvements
- Loss due to the outage of public utilities you rely on (e.g., local power company)

It is critical that you review the terms and conditions of your policy and understand all applicable coverages and exclusions. Periodic review of your policy and coverage is also recommended.

WHAT TO EXPECT IN THE UNDERWRITING PROCESS

Insurers use the underwriting process to assess your organization's risk and evaluate exposures. The process can also help you better understand your cyber risk profile relative to your peers and model losses. The application process typically involves a thorough assessment of the measures that your organization has in place to protect against cyber incidents and mitigate their impact. Water systems are also encouraged to take actions to reduce cyber risk, improve resilience to cyber incidents, and utilize free services (Top 8 Fact Sheet). Underwriting questionnaires are not harmonized across the industry, but insurers typically inquire about:

- Multi-Factor Authentication (MFA)
- Security awareness training and testing
- Data backups
- Endpoint detection and response/managed detection and response
- Vulnerability management (for computer and network security)
- Incident response and business continuity plans
- Third-party vendor management program

CISA Cybersecurity Resources

CISA Cybersecurity Resources

- CISA Regional Resources
- Cybersecurity Resources
  - CISA's Free Cyber Vulnerability Scanning for Water Utilities
  - 4 Things You Can Do To Keep Yourself Cyber Safe
  - Report to CISA
  - Cybersecurity Alerts & Advisories
  - Cyber Risks & Resources for the Water and Wastewater Systems Sector Infographics
  - Cross-Sector Cybersecurity Performance Goals
  - Known Exploited Vulnerabilities Catalog
  - CyberSentry Program
  - Logging Made Easy (LME)
  - Secure Our World
  - Industrial Control Systems Training
  - Known Exploited Vulnerabilities (KEV) Catalog

Wrap-Up

Poll 5

Conclusion

- Increase in frequency and severity of unauthorized remote access and ransomware attacks that result in impacts to operational and business systems at water and wastewater utilities.
  - Insider Threats, Social Engineering (including Phishing), Malware
- Attacks are increasingly malware-free and target internet-exposed devices with vulnerabilities.
- Cybersecurity best practices to secure IT and OT systems.
- Resources to protect against, and reduce impacts from, cyber threats.

Questions?

- https://www.epa.gov/cyberwater

Post-Course Questionnaire

- Let us know how we did!