Texas Water Systems Cybersecurity:

Texas Water and Wastewater Cybercrime Prevention, Response, and Recovery

Prepared and Presented by AIA Insurance Agency and the WinStar Insurance Group

Brett Cheatham, AIA Insurance Sales Manager
Mark Kaufman, AIA Insurance Sales Executive

INSURANCE AGENCY
A DIVISION OF WINSTAR INSURANCE GROUP

Texas Water Systems Cybersecurity

Presentation Outline

- Introduction
- Cybersecurity
- Cybercrime
- How to Prepare for a Cyber Incident
- How to Respond to a Cyber Incident
- How to Recover from a Cyber Incident
- TCEQ Cybercrime Reporting Requirements
- Texas Attorney General Data Breach Reporting Requirements
- CISA, EPA, and FBI: “Top Cyber Actions for Securing Water Systems”
- Conclusion

Introduction

Texas Water Systems Cybersecurity

Introduction

- AIA Insurance Agency is a full-service and independent Texas insurance agency dedicated to supporting Lone Star State water and wastewater service providers. Since 1978, AIA has specialized in creating customized insurance programs that ensure Texas water and wastewater systems operations run smoothly. AIA is a Texas Rural Water Association associate member and is endorsed by the Texas Rural Water Association (TRWA).

- The AIA Insurance program began in the mid-1980s to address the lack of management liability coverage for rural Texas water utilities. Over the years, AIA has expanded its insurance offerings to include tailored coverages for unique water and wastewater systems risks, making AIA the premier insurance provider for Texas water and wastewater utilities.

- AIA's knowledgeable insurance agents understand the Texas water and wastewater industry's specific needs, including how to mitigate cybersecurity risks, and are committed to delivering reliable and comprehensive insurance solutions for Texas' water utilities.

Texas Water Systems Cybersecurity

Introduction

INSURANCE AGENCY
A DIVISION OF WINSTAR INSURANCE GROUP

Texas Water Systems Cybersecurity

Introduction

Brett Cheatham
AIA North Region Sales Manager
940.230.5387
bcheatham@aiainsagency.com

Mark Kaufman
AIA South Region Sales Manager
601.415.2734
mkaufman@aiainsagency.com

INSURANCE AGENCY
A DIVISION OF WINSTAR INSURANCE GROUP

Texas Water Systems Cybersecurity

Introduction

- Clean and safe water is essential to human health and to local, state, and national economies
- Texas water and wastewater systems are critical infrastructure that face a multitude of cyberattack threats
- This presentation will provide cybersecurity guidance to help Texas water and wastewater system operators prevent, respond to, and recover from cyberthreats

Cybersecurity

Texas Water Systems Cybersecurity

Cybersecurity

- Cybersecurity- the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information

- Texas water systems cybersecurity is critical to protect Texas water and wastewater operations because these systems rely heavily on computers and the Internet to accomplish their missions

Texas Water Systems Cybersecurity

Cybersecurity

Cybersecurity helps protect Texas water and wastewater systems by:

- Safeguarding critical infrastructure
- Preserving the safety of public drinking water
- Protecting system financial solvency
- Avoiding legal liability issues
- Complying with government mandates
- Maintaining customer and public trust

Texas Water Systems Cybersecurity

Cybersecurity

Texas Water Systems Cybersecurity

Cybersecurity

Texas Water Systems Cybersecurity

Cybersecurity

Texas Water Systems Cybersecurity

Cybersecurity

- ***May 21, 2024, NBC News Report***

https://www.nbcnews.com/tech/security/us-says-cyberattacks-water-supplies-are-rising-rcna153280

INSURANCE AGENCY
A DIVISION OF WINSTAR INSURANCE GROUP

Texas Water Systems Cybersecurity

Cybersecurity

Russia-linked hacking group suspected of carrying out cyberattack on Texas water facility, cybersecurity firm says

By Sean Lyngaas, CNN
5 minute read · Published 6:07 AM EDT, Wed April 17, 2024

(CNN) — A hacking group with ties to the Russian government is suspected of carrying out a cyberattack in January that caused a tank at a Texas water facility to overflow, experts from US cybersecurity firm Mandiant said Wednesday.

The hack in the small town of Muleshoe, in north Texas, coincided with at least two other towns in north Texas taking precautionary defensive measures after detecting suspicious cyber activity on their networks, town officials told CNN. The FBI has been investigating the hacking activity, one of the officials said.

Texas Water Systems Cybersecurity

Cybersecurity

EPA urges water utilities to protect nation's drinking water amid heightened cyberattacks

Thao Nguyen
USA TODAY

Published 12:04 a.m. ET May 21, 2024 | **Updated 12:57 p.m. ET May 21, 2024**

EPA issues cyberattack warning for water utilities

The Environmental Protection Agency issued a countrywide alert urging water utilities to take immediate action to safeguard drinking water from cyberattacks. *Wibbitz - News*

https://www.usatoday.com/videos/news/2024/05/21/epa-warns-of-cyberattacks-on-us-water-systems/73786911007/

INSURANCE AGENCY
A DIVISION OF WINSTAR INSURANCE GROUP

Texas Water Systems Cybersecurity

Cybersecurity

Cybersecurity Methods

- Strong Passwords
- Email Security Tools
- Antivirus Software
- Firewalls
- Virtual Private Networks (VPNs)
- Multi-Factor Authentication
- Cyber Security Awareness Training
- Cyber Liability Insurance Coverage

Cybercrime

Texas Water Systems Cybersecurity

Cybercrime

- Cybercrime- criminal activities carried out using digital devices or networks
- Cybercrime involves using technology to commit fraud, identity theft, data breaches, and scams
- Cybercrime exploits vulnerabilities in computer systems and networks to gain unauthorized access; steal sensitive information; disrupt services; and cause financial or reputational harm to individuals, organizations, and governments

Texas Water Systems Cybersecurity

Cybercrime

- Water and wastewater computer and cyber systems are vulnerable to a wide range of hazards from both physical attacks and cyberthreats

- Cybercriminals exploit water and wastewater systems' cyber infrastructure vulnerabilities to steal information and money and to threaten the delivery of essential services such as purifying drinking water and treating wastewater

- Texas drinking water and wastewater utilities are critical enterprises that must evaluate and mitigate their vulnerability to cyber incidents to protect the health and safety of Texans

Texas Water Systems Cybersecurity

Cybercrime

Cybercrime affecting water and wastewater systems includes:

- Interruption of treatment, distribution, or conveyance processes
- Opening and closing valves
- Disabling pumps
- Stealing customer personal data
- Defacing websites
- Compromising email systems
- Damaging system components
- Losing use of industrial systems, such as the SCADA system

Texas Water Systems Cybersecurity

Cybercrime

- Cybercriminal- someone who uses technology to commit illegal and malicious activities on digital systems or networks with the intention to steal sensitive information, personal information, and money.

- 3 main types of cyber criminals:
  - Hackers
  - Nation-State Actors
  - Insiders

Texas Water Systems Cybersecurity

Cybercrime

- Hacker- a cybercriminal who uses computers to gain unauthorized access to data on a computer network or system

- Nation-State Actor- a cybercriminal funded by nation states and governments to steal sensitive data, gather confidential information, or disrupt critical infrastructure

- Insider- a cybercriminal who works for an organization affected by a cybercrime, including an employee, a former employee, a contractor, or a business associate

Texas Water Systems Cybersecurity

Cybercrime

Types of Cyberattacks:

- Malware
- Phishing
- Man-in-the-Middle Attack
- Denial-of-Service Attack
- Zero-Day Exploits
- Password Attack
- Internet of Things Attack
- Code Injection Attacks

Texas Water Systems Cybersecurity

Cybercrime

Malware

- Short for “malicious software”
- Software code written to intentionally harm a computer system or its users
- Used in almost every modern cyberattack
- Used to gain unauthorized access to a computer system to render it inoperable, destroy data, and steal sensitive data

Texas Water Systems Cybersecurity

Cybercrime

Malware Types

- Ransomware- locks a victim's data or device then requires the victim to pay ransom to the attacker to unlock the data or device
- Trojan horse - malicious code that tricks people to download it by appearing to be a useful program or hiding within legitimate software
- Spyware- highly secretive malware that gathers and sends to the attacker sensitive information such as usernames, passwords, and banking data
- Worm- a self-replicating program that automatically spreads to apps and devices without human interaction

Texas Water Systems Cybersecurity

Cybercrime

Phishing

- A form of social engineering known as “human hacking” that manipulates targets into taking actions to expose confidential information, threaten their organization’s financial well-being, and compromise organizational security

- Uses fraudulent email messages, email attachments, text messages, web sites, and phone calls to trick people into sharing personal data or login credentials, downloading malware, and sending money to cybercriminals

Texas Water Systems Cybersecurity

Cybercrime

Phishing Types

- Spear phishing- highly-targeted phishing attacks that manipulate a specific individual using details from the victim's public social media profiles

- Whale phishing – spear fishing that targets corporate executives or wealthy individuals

- Business email compromise (BEC)- scams in which cybercriminals pose as executives, vendors, or trusted business associates to trick victims into wiring money or sharing sensitive data

Texas Water Systems Cybersecurity

Cybercrime

Cyberattack Types

- Man-in-the-Middle Attack
- Denial-of-Service Attack
- Zero-Day Exploits
- Password Attack
- Internet of Things Attack
- Code Injection Attack

Texas Water Systems Cybersecurity

Cybercrime

Man-in-the-Middle Attack

- A cybercriminal eavesdrops on a network connection to intercept and relay messages between two parties and steal data

- Typically occurs on unsecured Wi-Fi wireless networks

Texas Water Systems Cybersecurity

Cybercrime

Denial-of-Service Attack

- Overwhelms a website, application, or system with volumes of fraudulent traffic, making it too slow to use or entirely unavailable to legitimate users

- A distributed denial-of-service attack is similar and uses a network of Internet-connected, malware-infected devices or bots (botnet) to cripple or crash a system

Texas Water Systems Cybersecurity

Cybercrime

Zero-Day Exploits

- Takes advantage of an unknown, unaddressed, or unpatched security flaw in computer software, hardware, or firmware

- “Zero Day” refers to the fact that a software or device has no time to fix the vulnerabilities because malicious actors can already use them to gain access to vulnerable systems

Texas Water Systems Cybersecurity

Cybercrime

Password Attack

- Cybercriminals try to guess or steal the password or login credentials to a user's account

- These often occur using social engineering to trick victims to unwittingly share their password or login credentials

Texas Water Systems Cybersecurity

Cybercrime

Internet of Things Attack

- Internet of Things (IoT)- a collective network of connected devices and technology that facilitates communication between devices and the cloud, and between the devices themselves
- The four main types of IoT are consumer, commercial, industrial, and infrastructure
- Each type of IoT serves a distinctive purpose such as enhancing everyday life, optimizing industrial processes, and managing urban infrastructure
- Cybercriminals take over an IoT device to steal data or use the device as part of a botnet for other malicious activity

Texas Water Systems Cybersecurity

Cybercrime

Code Injection Attack

- Hackers inject malicious code into a program or download malware to execute remote commands that allow them to read or modify a database or to change website data
- A structured query language (SQL) injection attack is where hackers exploit the SQL syntax--the standard computer language for accessing and manipulating data--to spoof identity; expose, tamper, destroy, or make existing data unavailable; or become the database server administrator
- Cross-Site Scripting (XSS) infect users who visit a website and then extract data from the infected devices

How to Prepare for a Cyber Incident

Texas Water Systems Cybersecurity

How to Prepare for a Cyber Incident

- Identify all mission-critical information technology (IT) systems related to business enterprise, process control, and communications
- Identify the personnel or entities responsible for operating and maintaining each mission-critical IT system
- Identify an overall information technology (IT) security lead to oversee all cyber-related duties

Texas Water Systems Cybersecurity

How to Prepare for a Cyber Incident

- Identify points of contact for reporting cyber incidents and requesting assistance with response and recovery

- Develop, regularly review, and periodically update an emergency response plan (ERP) to address reacting to a cyber incident impacting business enterprise, process control, and communication systems

- Train all essential personnel to perform mission-critical functions during a cyber incident that disables business enterprise, process control, and communication systems

Texas Water Systems Cybersecurity

How to Prepare for a Cyber Incident

- Establish a program to maintain updated anti-virus software on all critical IT systems and to install security patches
- Automatically back up critical IT systems and ensure the process produces a readable and uncorrupted restore file
- Implement rigorous user authentication including multi-factor authentication

Texas Water Systems Cybersecurity

How to Prepare for a Cyber Incident

- Use tools and subject-matter experts provided by the U.S. government
  - Cybersecurity and Infrastructure Security Agency (CISA): https://www.cisa.gov/cybersecurity
  - Environmental Protection Agency (EPA): https://public.govdelivery.com/accounts/USEPAOGWDW/subscriber/new?qsp=USEPAOGWDW_1
  - Cybersecurity and Infrastructure Security Agency (CISA): https://public.govdelivery.com/accounts/USDHSCISA/subscriber/new?qsp=CODE_RED
  - Federal Bureau of Investigation (FBI): https://www.ic3.gov/Home/IndustryAlerts

How to Respond to a Cyber Incident

Texas Water Systems Cybersecurity

How to Respond to a Cyber Incident

- Disconnect compromised computers from the network to isolate breached components and prevent further damage
- Do not turn off or reboot information technology (IT) systems to preserve evidence and allow for an IT assessment of the cyberthreat
- Notify IT personnel about the incident and request for emergency response assistance

Texas Water Systems Cybersecurity

How to Respond to a Cyber Incident

- Assess any damage to utility system equipment

- Assess any utility operations disruptions

- Execute the utility emergency response plan (ERP)
  - ➢ Notify utility personnel
  - ➢ Restore mission critical operations processes
  - ➢ Make proper public notification

Texas Water Systems Cybersecurity

How to Respond to a Cyber Incident

- Report the cyber incident to law enforcement, regulatory agencies, and insurance company

- Notify external entities that may have remote connections to the affected network

- Document key incident information
  - Suspicious phone calls, emails, or messages
  - Damage to utility systems
  - Steps taken to respond to the incident and when they were taken

How to Recover from a Cyber Incident

Texas Water Systems Cybersecurity

How to Recover from a Cyber Incident

- Work with information technology (IT) staff, vendors, government partners, and your insurance company to obtain resources and assistance needed for recovery

- Notify affected employees and customers of any personally identifiable information (PII) that was compromised

- Submit an incident report through WaterISAC--a non-profit organization that provides information about water security and threats--at 866.H2O.ISAC (866.426.4722) or www.waterisac.org

Texas Water Systems Cybersecurity

How to Recover from a Cyber Incident

- Develop a lessons-learned document and an after-action report (AAR) to document utility response activities, successes, and improvement areas
- Create an improvement plan (IP) based on your AAR analysis
- Use the IP to update your vulnerability assessment, emergency response plan (ERP), and contingency plans

TCEQ Cybercrime Reporting Requirements

Texas Water Systems Cybersecurity

TCEQ Cybercrime Reporting Requirements

- The Texas Commission on Environmental Quality (TCEQ) is responsible for enforcing rules about Texas public water systems

- The TCEQ rules in 30 Texas Administrative Code, Chapter 290, Subchapter D, Rules and Regulations for Public Water Systems specify water treatment plant design, operation, and maintenance requirements for public water systems

Texas Water Systems Cybersecurity

TCEQ Cybercrime Reporting Requirements

- Texas Commission on Environmental Quality (TCEQ) rule Section 290.46(w), Security, of 30 Texas Administrative Code, Chapter 290, Subchapter D, Rules and Regulations for Public Water Systems requires Texas water systems to report various water facility security events

- This rule requires all Texas water systems to notify the TCEQ executive director by a toll-free reporting phone number ***immediately*** of certain water facility security events that may negatively impact the production or delivery of safe and adequate drinking water

Texas Water Systems Cybersecurity

TCEQ Cybercrime Reporting Requirements

- Water facility security events that must be reported to the Texas Commission on Environmental Quality (TCEQ) immediately are:
  - An unusual or unexplained authorization entry at public water system property
  - An act of terrorism against the public water system
  - An unauthorized attempt to probe for or gain access to proprietary information that supports the key activities of the public water system
  - A theft of property that supports the public water system's key activities
  - A natural disaster, accident, or act that results in public water system damage

Texas Water Systems Cybersecurity

TCEQ Cybercrime Reporting Requirements

- This water facility security events under Section 290.46(w) must be reported immediately to the Texas Commission on Environmental Quality (TCEQ) on the Water/Wastewater Homeland Security Threat Hotline at 888.777.3186

- This phone number is found on the TCEQ Toll-free Numbers website at https://www.tceq.texas.gov/agency/directory/tollfree.html

Texas Water Systems Cybersecurity

TCEQ Cybercrime Reporting Requirements

Home / Agency / Directory / TCEQ Toll-free Numbers

Questions or Comments:
info@tceq.texas.gov

TCEQ Toll-free Numbers

The TCEQ makes several 800, 888, 877, 866, and 855 phone numbers available for specific information and reporting lines.

Please note that calls cannot be transferred to other areas of the agency from these connections.

The TCEQ does not have a general toll-free number. The main switchboard can be contacted by dialing 512-239-1000.

Water/Wastewater Homeland Security Threat Hot Line:
888-777-3186
Water and wastewater systems are required to report acts that threaten the ability of their system to provide safe and adequate water and wastewater services. Calls are routed automatically to the closest TCEQ regional office. After business hours, callers may leave a recorded message or may be forwarded to an after-hours pager or answering service.

Texas Attorney General Data Breach Reporting Requirement

Texas Water Systems Cybersecurity

Texas Attorney General Data Breach Reporting Requirement

- House Bill 4390 was enacted in 2019 by the 86th Texas Legislature to require a person who conducts business in Texas that includes sensitive personal information to report to the Texas Attorney General certain data breaches within 60 days of identifying the breach

- HB 4390 requires reporting to the Attorney General disclosures of system security breaches in which an individual's sensitive personal information was or was reasonably believed to have been acquired by an authorized person

Texas Water Systems Cybersecurity

Texas Attorney General Data Breach Reporting Requirement

- HB 4390 also required a person or entity who owned or licensed the data including sensitive personal information that was the subject of the security breach to notify the attorney general of the breach if it involved 250 or more state residents

- The goal of HB 4390 was to strengthen notification requirements in the case of a security breach affecting sensitive personal information to better protect individuals from potential harm caused by a security breach

Texas Water Systems Cybersecurity

Texas Attorney General Data Breach Reporting Requirement

The HB 4390 notification must include:

- a detailed description of the nature and circumstances of the breach or the use of sensitive information acquired as a result
- the number of Texas residents affected
- measures taken by the person or entity regarding the breach
- any measures that the person or entity intended to take regarding the breach after the notification
- information on whether law enforcement was engaged in investigating the breach

Texas Water Systems Cybersecurity

Texas Attorney General Data Breach Reporting Requirement

- The 88th Texas Legislature in 2023 amended the HB 4390 law through enactment of Senate Bill 768 to:

  - Decrease from 60 days to 30 days the requirement for when businesses must notify the attorney general of any data breach involving at least 250 Texas residents

  - Require electronic reporting of data breaches to the Texas Attorney General

Texas Water Systems Cybersecurity

Texas Attorney General Data Breach Reporting Requirement

- HB 4390 and SB 768 data breach reporting can be completed on the Texas Attorney General's website at https://www.texasattorneygeneral.gov/consumer-protection/data-breach-reporting

Texas Water Systems Cybersecurity

Texas Attorney General Data Breach Reporting Requirement

CISA, EPA, and FBI: "Top Cyber Actions for Securing Water Systems"

Texas Water Systems Cybersecurity

CISA, EPA, and FBI:
"Top Cyber Actions for Securing Water Systems"

- The U.S. Cybersecurity and Infrastructure Security Agency (CISA), the U.S. Environmental Protection Agency (EPA), and the U.S. Federal Bureau of Investigation (FBI) in February 2024 released a joint fact sheet outlining the cyber actions that water and wastewater sector entities can take to reduce risk and improve resilience to malicious cyber activity reduce overall vulnerability

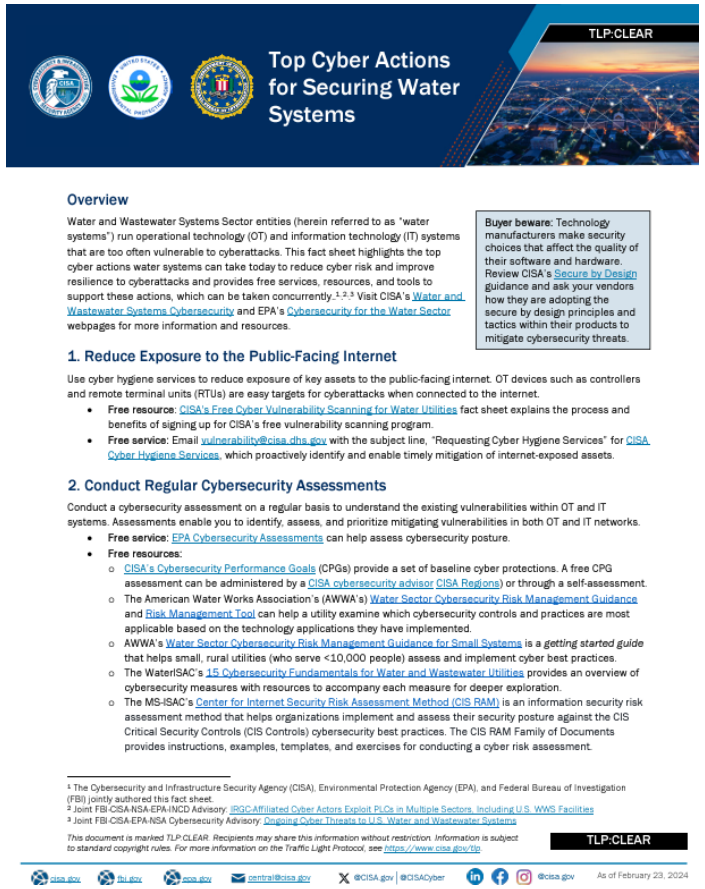
- The joint fact sheet is available on the CISA website at https://www.cisa.gov/resources-tools/resources/top-cyber-actions-securing-water-systems and is summarized on the Texas Department of Information Resources (DIR) website's Information Security section

- Additional support for implementing any of the actions outlined in the fact sheet is available from the EPA and CISA

Texas Water Systems Cybersecurity

CISA, EPA, and FBI:

"Top Cyber Actions for Securing Water Systems"



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.

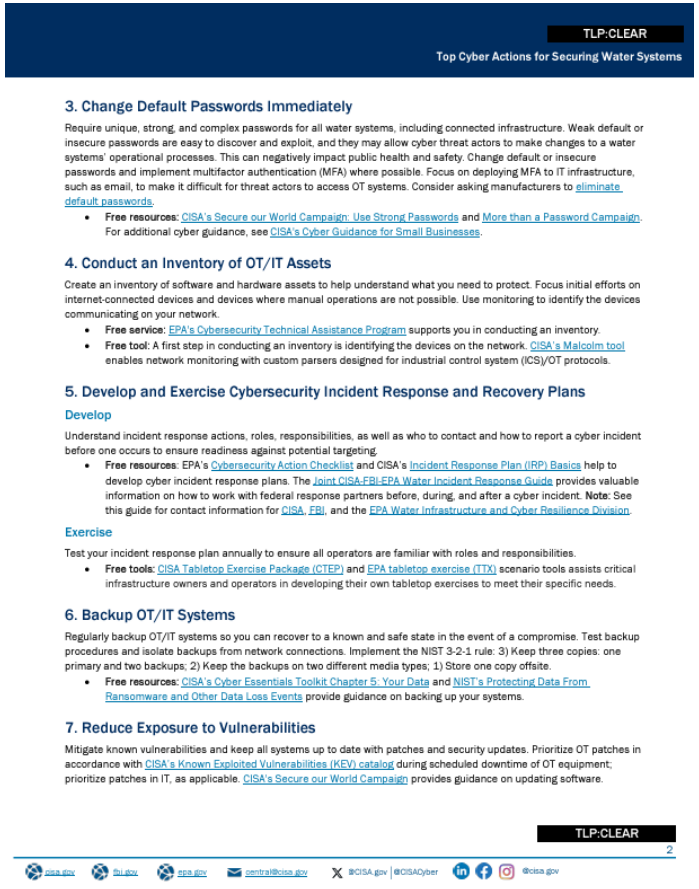
2. Conduct Regular Cybersecurity Assessments

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

TLP:CLEAR



3. Change Default Passwords Immediately

Require unique, strong, and complex passwords for all water systems, including connected infrastructure. Weak default or insecure passwords are easy to discover and exploit, and they may allow cyber threat actors to make changes to a water systems' operational processes. This can negatively impact public health and safety. Change default or insecure passwords and implement multifactor authentication (MFA) where possible. Focus on deploying MFA to IT infrastructure, such as email, to make it difficult for threat actors to access OT systems. Consider asking manufacturers to eliminate default passwords.

- **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

Create an inventory of software and hardware assets to help understand what you need to protect. Focus initial efforts on internet-connected devices and devices where manual operations are not possible. Use monitoring to identify the devices communicating on your network.

- **Free service:** EPA's Cybersecurity Technical Assistance Program supports you in conducting an inventory.
- **Free tool:** A first step in conducting an inventory is identifying the devices on the network. CISA's Malcolm tool enables network monitoring with custom parsers designed for industrial control system (ICS)/OT protocols.

5. Develop and Exercise Cybersecurity Incident Response and Recovery Plans

Develop

Understand incident response actions, roles, responsibilities, as well as who to contact and how to report a cyber incident before one occurs to ensure readiness against potential targeting.

- **Free resources**: EPA's Cybersecurity Action Checklist and CISA's Incident Response Plan (IRP) Basics help to develop cyber incident response plans. The Joint CISA-FBI-EPA Water Incident Response Guide provides valuable information on how to work with federal response partners before, during, and after a cyber incident. **Note:** See this guide for contact information for CISA, FBI, and the EPA Water Infrastructure and Cyber Resilience Division.

Exercise

Test your incident response plan annually to ensure all operators are familiar with roles and responsibilities.

- **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

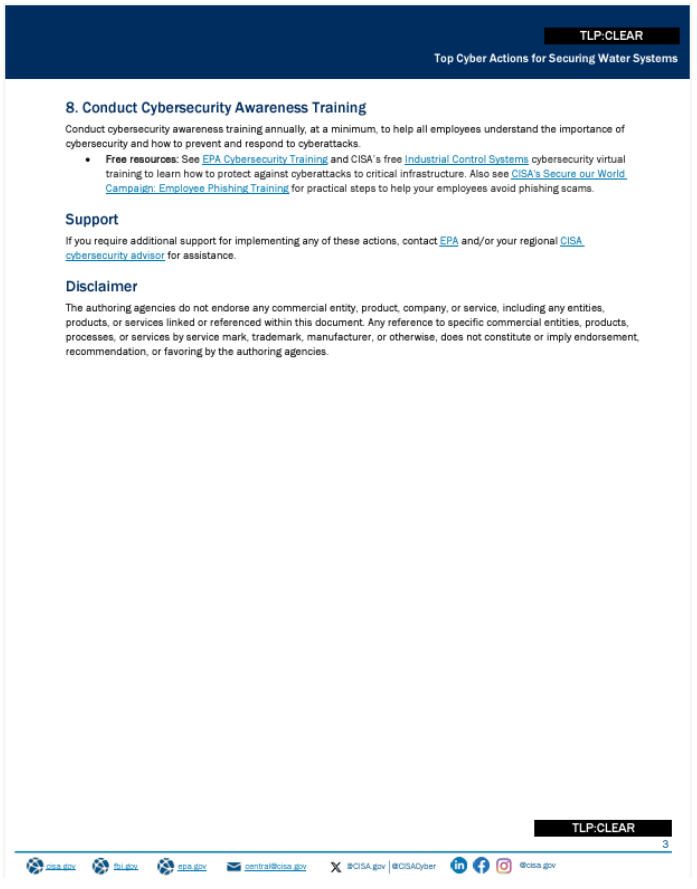
Regularly backup OT/IT systems so you can recover to a known and safe state in the event of a compromise. Test backup procedures and isolate backups from network connections. Implement the NIST 3-2-1 rule: 3) Keep three copies: one primary and two backups; 2) Keep the backups on two different media types; 1) Store one copy offsite.

- **Free resources:** CISA's Cyber Essentials Toolkit Chapter 5: Your Data and NIST's Protecting Data From Ransomware and Other Data Loss Events provide guidance on backing up your systems.

7. Reduce Exposure to Vulnerabilities

Mitigate known vulnerabilities and 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 equipment; prioritize patches in IT, as applicable. CISA's Secure our World Campaign provides guidance on updating software.

TLP:CLEAR



8. Conduct Cybersecurity Awareness Training

Conduct cybersecurity awareness training annually, at a minimum, 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. Also see CISA's Secure our World Campaign: Employee Phishing Training for practical steps to help your employees avoid phishing scams.

Support

If you require additional support for implementing any of these actions, contact EPA and/or your regional CISA cybersecurity advisor for assistance.

Disclaimer

The authoring agencies do not endorse any commercial entity, product, company, or service, including any entities, products, or services linked or referenced within this document. Any reference to specific commercial entities, products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply endorsement, recommendation, or favoring by the authoring agencies.

TLP:CLEAR

Texas Water Systems Cybersecurity

CISA, EPA, and FBI:
"Top Cyber Actions for Securing Water Systems"

- The three-page joint fact sheet--co-sealed by the CISA, EPA, and FBI--outlines the following cyber actions water and wastewater systems sector entities can take to reduce risk and improve resilience to malicious cyber activity and provides free services, resources, and tools to support these actions:

  - Reduce exposure to the public-facing Internet
  - Conduct regular cybersecurity assessments
  - Change default passwords immediately
  - Conduct an inventory of operational technology (OT)/information technology (IT) assets
  - Develop and exercise cybersecurity incident response and recovery plans
  - Backup OT/IT Systems
  - Reduce exposure to vulnerabilities
  - Conduct cybersecurity awareness training

Texas Water Systems Cybersecurity

CISA, EPA, and FBI:
"Top Cyber Actions for Securing Water Systems"

- **Reduce Exposure to the Public-Facing Internet**
  - Use cyber-hygiene services to reduce exposure of key assets to the public-facing Internet

- **Conduct Regular Cybersecurity Assessments**
  - Conduct a cybersecurity assessment on a regular basis to understand and prioritize existing vulnerabilities

- **Change Default Passwords Immediately**
  - Require unique, strong, and complex passwords for all water systems, including connected infrastructure
  - Do not use default passwords
  - Implement multi-factor authentication (MFA)

Texas Water Systems Cybersecurity

CISA, EPA, and FBI:
"Top Cyber Actions for Securing Water Systems"

- **Conduct an Inventory of Operational Technology (OT)/Information Technology (IT) Assets**
  - Create an inventory of software and hardware assets to help the security team understand what needs to be protected

- **Develop and Exercise Cybersecurity Incident Response and Recovery Plans**
  - Develop and exercise cybersecurity incident response and recovery plans
  - Include in the plans defined incident response actions, roles, and responsibilities, as well as who to contact and how to report a cyber incident

- **Backup Operational Technology (OT)/Information Technology (IT) Systems**
  - Regularly backup OT/IT systems so they can be recovered to a known and safe state in the event of a compromise
  - Test backup procedures and isolate backups from network connections

Texas Water Systems Cybersecurity

CISA, EPA, and FBI:
"Top Cyber Actions for Securing Water Systems"

- **Reduce Exposure to Vulnerabilities**
  - Mitigate known vulnerabilities, especially known exploited vulnerabilities
  - Keep all systems updated with patches and security updates

- **Conduct Cybersecurity Awareness Training**
  - Train all employees at least annually on cybersecurity awareness
  - Ensure the training explains how to prevent and respond to cyberattacks

Conclusion

Texas Water Systems Cybersecurity

Conclusion

- Clean and safe water is essential to human health and to local, state, and national economies
- Texas water and wastewater systems are critical infrastructure that face a multitude of cyberattack threats
- This presentation has provided cybersecurity guidance to help Texas water and wastewater system operators assess cyberthreats to their systems and identify ways to prepare for, respond to, and recover from cyberthreats to their systems

Texas Water Systems Cybersecurity

Conclusion

Questions?