

Tennessee Association
of Utility Districts

Vital for Tennessee's future



CYBERSECURITY WORKSHOP

DECEMBER 5, 2024

David Money

davidmoney@taud.org

931-477-0963

Greg Baker

gregbaker@taud.org

731-225-5240

Cyber Security Basics

- Asset inventory- identify vulnerabilities
- Take mitigating actions- Firewalls software updates- training staff
- Back up critical data
- Develop a response plan in case of attack

Cyber Security



February 5, 2021 unauthorized access to SCADA system at a Water Treatment Facility in Oldsmar, FL

- Took control of the Caustic Feed controls and increased feed rate.
- WTP was using Windows 7, no security updates
- Access was gained through Team Sharing software

March 12, 2021- unauthorized access to a TN Water System through Microsoft Exchange.

- No indication of control access.



Cyber Security

May 7, 2021 -DarkSide ransomware infiltrates colonial gas pipeline systems used to operate pipelines.

- Company paid a \$5M ransom
- Used its own back up data for operations restoration.

```
script src=[true]local.config (245,23,068,789,a48) [lock.command]#>>access:status [true]
function login.credentials {
  name<img>=s
  ess:logged<[if]net.log.origin.set(278,56,34,)#>>
  e[get]script src=(#wack %$%#m#e#o#)
  a?/q/s) {logged=online.click}
  logger.warning) #key_input <chain>= (d fg#s m#e#
  e) add.string<status> (<a3*s=w90t8l2)
  n) local.config status=[error]
  n) local.config status=[error]
  status=[error]
  ess:status [true]
  .log.origin set (278,56,34,)#>>[if] #Frame<img>=span
  .click)
  Key_input<img>=span
  status=[error]
  ss=s[error]
  og.origin
  src=(#wack %$%#m#e#o#)
  logged=online.click
  r.warning) #key_input <chain>= (d fg#s m#e#
  ) add.string<status> (<a3*s=w90t8l2)
  n) local.config status=[error]
  n) local.config status=[error]
  (7u nown) local.config status=[error]
  d.string<status> (<a3*s=w90t8l2)
  m nd]#>>access:status [true]
  s og ed<[if]net.log.origin.set(278,56,34,)#>>
  q s an a dr
```



December 16, 2021, the Cybersecurity and Infrastructure Security Agency (CISA), FBI, and the National Security Agency issued a joint advisory on Russian state-sponsored cyber operations against United States critical infrastructure

- EPA emailed information and advisory to 8000 System.

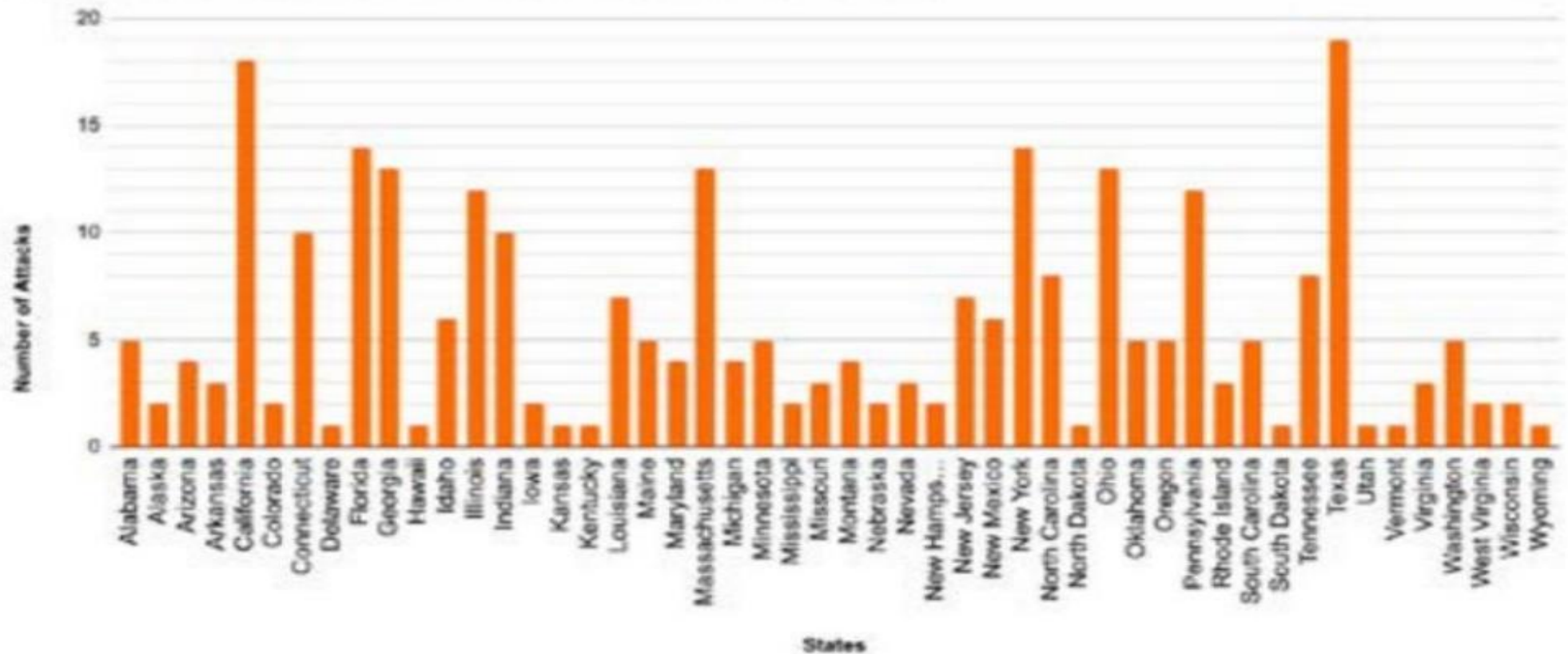
Cyber Security

Cyber-attacks on Municipalities



FEMA

Ransomware Attacks On State Municipalities (2013-2020)





COT Cyber Aware

Ransomware Attack Hits 22 Texas Towns, Authorities Say

After crippling ransomware attack, Baltimore council members look for answers

Watch later

Share

Johnson City targeted in ransomware attack

Spring Hill, Tenn., Hit with Ransomware Attack

The FBI is investigating a ransomware attack on the city of Atlanta

MORE VIDEOS

FBI investigating after Collierville hit by ransomware attack. Here's what you need to know



1:21 / 2:13



YouTube





```

11000100 01000011 01110111 11100011 11111000 11010011 11001010 10100111
11010101 10101100 00111100 11101110 01110100 00001100 10111111 10100000
11100011 01000111 01001101 01100011 01100111 10100110 01100011 00101001
1001010

```


Major Cyber Threats To Critical Infrastructure

Ransomware:

- Ransomware is a form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable
 - Medusa (ransomware as a service)
 - Clop

Hacktivists

- A hacktivist is someone who uses hacking to bring about political and social change.

Information Technology / Operational Technology Convergence:

- IT/OT convergence is the integration of information technology (IT) systems with operational technology (OT) systems. IT systems are used for data-centric computing and typically are business systems; OT systems monitor events, processes and devices, and make adjustments in enterprise and industrial operations.



EPA Cyber Security Assessment Tool Tech definitions

- **Information Technology- (IT)**- A set of resources that an organization uses for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information
- **Operational Technology (OT)** -hardware and software that detects or causes a change through the direct monitoring or control of physical devices, processes, and events in the enterprise- examples would be Industrial Control Systems (ICS) or SCADA, PLCs (programmable logic controllers, RTUs (Remote Terminal Unit), HMI (user interface or dashboard)
- https://www.epa.gov/system/files/documents/2024-03/assessing-if-a-wws-has-ot_508_c.pdf

Industrial Control Systems (ICS)

Industrial Control Systems (ICS) ICS are ;

- A category of Operational Technology (OT) that focus on automating or remotely controlling physical processes.
- This is in contrast to Information Technology (IT), which focuses on manipulating, recording, and conveying data.

Supervisory Control and Data Acquisition (SCADA) systems

Large-scale distributed measurement and control systems designed to collect field information, transfer it to a control center, and display the information for monitoring.

SCADA systems are used in the transmission and distribution of electricity, gas, oil, and water.

Human Machine Interface (HMI)

- **Is a graphical control panel that displays different functions and data elements of ICS for human review and control.**

Programmable Logic Controller (PLC)

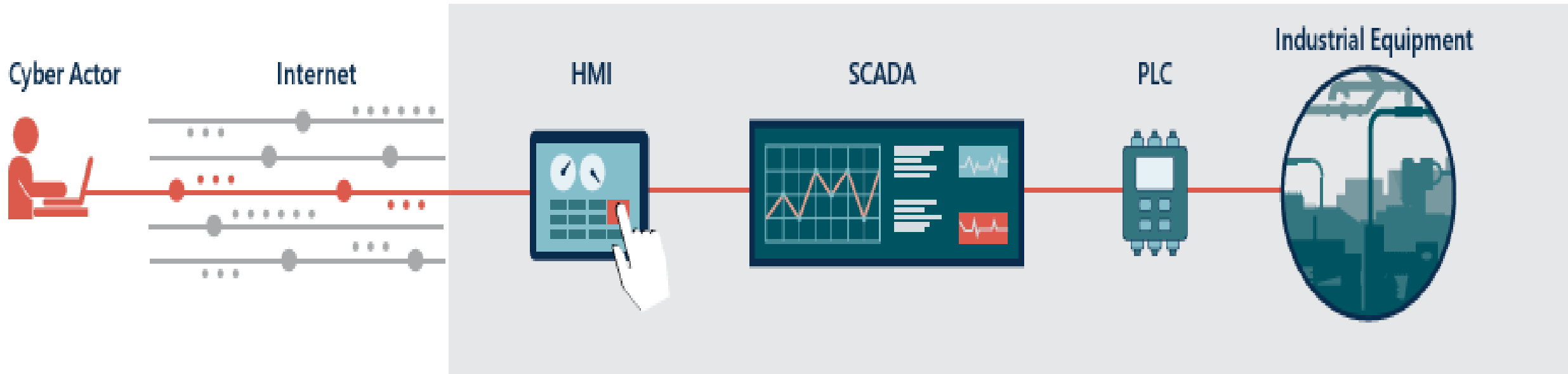
- **A small industrial computer responsible for executing specific physical subprocesses, such as logic, timing, counting, communication, and data and file processing.**

Remote Terminal Unit (RTU)

- **A control device typically installed in a remote location as part of a larger system. The main purpose of an RTU is to monitor and control field devices, such as valves, actuators, sensors, and more.**

Industrial Control Systems Infrastructure

CYBER ACTOR ATTACKS ICS INFRASTRUCTURE



Why and Who would attack Water/Wastewater Systems

- **Why? WWS Is An Easy Target and Demands Attention**

- IT/OT convergence increases threat attack surface
- Typically, low cybersecurity resources.
- Poor cyber hygiene and network segmentation

- **Who? Anyone, Anybody**

- Strong organized state actors attempting to disrupt our way of life
- Mid to low level criminals looking for a quick buck or make a political statement
- Insider threats from accidental everyday operations to disgruntle employees



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

The U.S. authoring agencies have confirmed that Volt Typhoon has compromised the IT environments of multiple critical infrastructure organizations—primarily in [Communications](#), [Energy](#), [Transportation Systems](#), and [Water and Wastewater Systems](#) Sectors—in the continental and non-continental United States and its territories, including Guam. Volt Typhoon’s choice of targets and pattern of behavior is not consistent with traditional cyber espionage or intelligence gathering operations, and the U.S. authoring agencies assess with high confidence that Volt Typhoon actors are pre-positioning themselves on IT networks to enable lateral movement to OT assets to disrupt functions.

Exploitation of Unitronics PLCs used in Water and Wastewater Systems

Change all default passwords on PLCs and HMIs and use a [strong password](#). Ensure the Unitronics PLC default password “1111” is not in use.



IRGC-affiliated cyber actors using the persona “CyberAv3ngers” are actively targeting and compromising Israeli-made Unitronics Vision Series PLCs that are publicly exposed to the internet, through the use of default passwords. The PLCs may be rebranded and appear as different manufacturers and company names.

YOU HAVE BEEN
HACKED

DOWN WITH ISRAEL الموت لإسرائيل

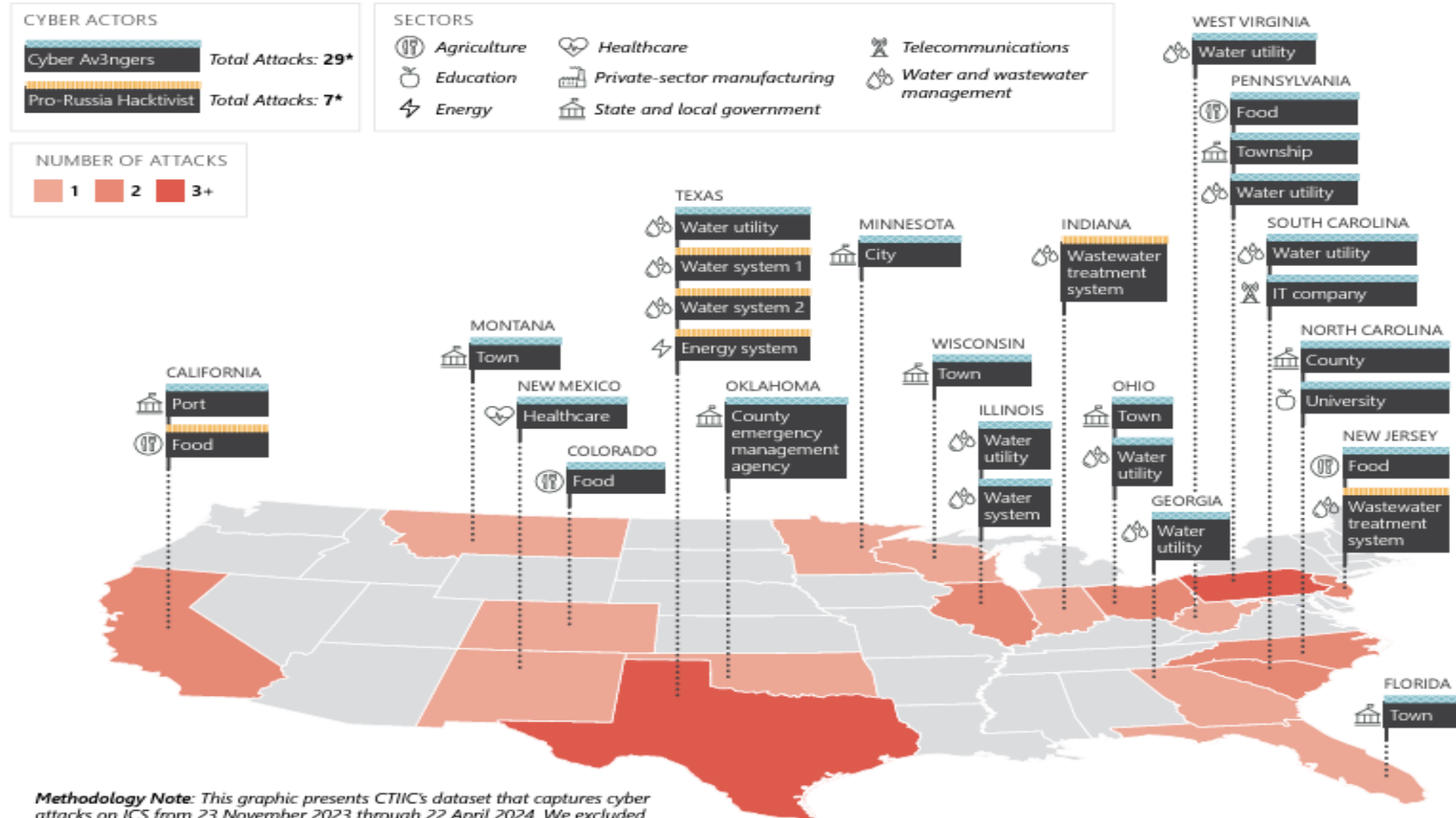


EVERY EQUIPMENT
"MADE IN ISRAEL"
IS CYBER AV3NGERS
LEGAL TARGET



US ICS attacks Nov 23- April 24

REPORTED CYBER ATTACKS ON US ICS, 23 NOVEMBER 2023 THROUGH 22 APRIL 2024



Methodology Note: This graphic presents CTIC's dataset that captures cyber attacks on ICS from 23 November 2023 through 22 April 2024. We excluded ransomware attacks on critical infrastructure entities.

*Including seven attacks at additional US locations.

In November 2023, Iranian-backed hackers gained access to one of the booster stations of Aliquippa, PA. The hackers took control of the critical node - which controls a group of booster pumps - before municipal officials were alerted by alarm.

Earlier this year (2024), the EPA warned nationwide water utilities of the increasing risk, and frequency, of cyberattacks on water systems. According to the agency, over 70% of water systems inspected by officials were not in compliance with common cybersecurity standards. U.S. officials have specifically targeted a Chinese-linked cyber threat known as Volt Typhoon, which continues to compromise information technology across the American critical infrastructure network.

Experts believe that Volt Typhoon is an adversarial strategy to pre-position on U.S. and allied IT infrastructure, in anticipation of launching cyberattacks in the event of conflict over Taiwan or another critical geopolitical issue.

April 2024 , three rural towns in Texas were attacked by a Russian hacktivist group. Over the course of four days, the town of Hale Center experienced 37,000 attacks on their firewall. In nearby Muleshoe, hackers caused the water system to overflow before officials managed to stem the flow manually.

- **February 2024, Middle TN water system**

- Impacted secondary SCADA computer, sluggishness
- Computer shutting on and off, unable to timestamp data
- Password may have allowed easy access

- **April 2024, Middle TN water system**

- Two of four filters drained after rate of flow controllers were adjusted to 100%, opened by outside entity
- Control panel was unresponsive and had to close valves manually





When are you coming in today?



Bob Freudenthal <executivedirector2366@gmail.com>

To: Greg Baker



Reply




Reply All



Forward



Tue 6/6/2023 5:54 AM

 If there are problems with how this message is displayed, click here to view it in a web browser.

CAUTION: This email originated from outside of the company. Do not click links or open attachments unless you recognize the sender and know the content is safe.

DM

David Money

From :Xianfang218@mail.com

To: ✓ David Money

Tue 12/3/2024 2:16 PM

U.S. Post: You have a USPS parcel being cleared, due to the detection of an invalid zip code address, the parcel can not be cleared, the parcel is temporarily detained, please confirm the zip code address information in the link with in 24 hours.

<https://p.updateinfoa.top/us>

(Please reply with a Y, then exit the text message and open it again to activate the link, or copy the link into your Safari browser and open it)

Have a great day from the USPS team!


Sent from my iPhone



Water Sector Cybersecurity Program Case Studies

Case Studies that highlight the cybersecurity programs implemented at utilities of all sizes:

- [Small Combined System](#)
- [Small Wastewater System](#)
- [Medium Drinking Water System](#)
- [Medium Drinking Water System #2](#)
- [Medium Combined System](#)
- [Large Combined System](#)



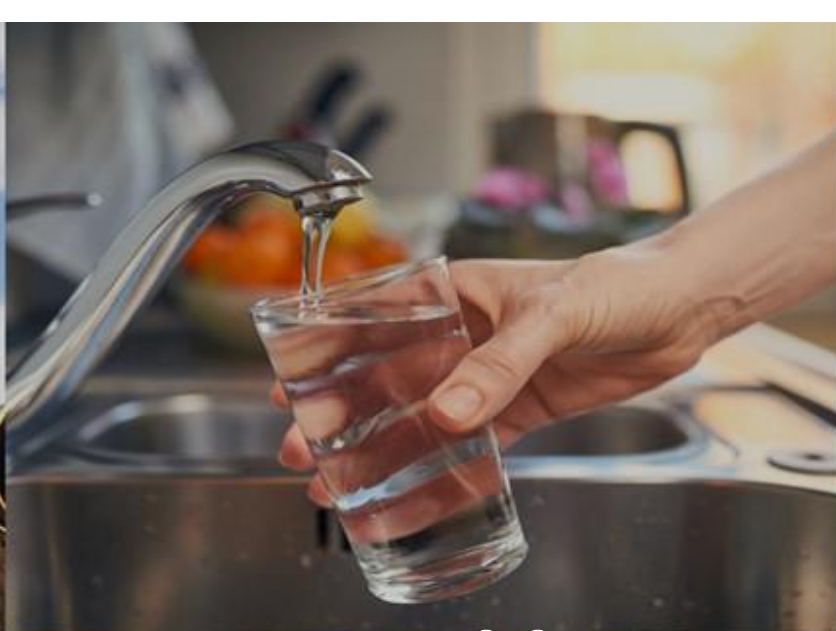
WATER SECTOR CYBERSECURITY PROGRAM
CASE STUDY: *Small Wastewater System*
Asset Inventory: A Good First Step to Balancing Risks

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 <ul style="list-style-type: none">• Separate standard user and privileged accounts• Password length requirements• Secure remote access policy	RESPONSE AND RECOVERY <ul style="list-style-type: none">• 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
DEVICE SECURITY <ul style="list-style-type: none">• OT and IT network asset inventory	
DATA SECURITY <ul style="list-style-type: none">• Log collection and monitoring frequency for intrusion detection	
VULNERABILITY MANAGEMENT <ul style="list-style-type: none">• OT asset connection to the public Internet	OTHER <ul style="list-style-type: none">• 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.



Cybersecurity Tabletop Exercise



Scenario

Inject #1 – Day 1, 2:25 PM

John, a new office clerk in the public utility office for the suburban town of Kingsburg receives an email from an unknown sender with the subject title “FedEx: Failed Package Delivery Notice.” Thinking he missed a package delivery; John opens the email.

When John opened the email, he noticed that “The Town of Kingsburg” was in the body and saw a PDF attachment. He opened the attachment to find out more information. The attachment looked generic and only stated that he missed package delivery, but they would try again tomorrow.

Lacking any further information on the package, he closed the email assuming whatever it was would just be delivered late.

Discussion

Is there anything suspicious about this email? If yes, what are some details that would increase your suspicion?

What would you do if you were in John's position?

Does your utility/organization have guidance or procedures that cover this type of situation?

Are your employees trained on what to do if they think they have experienced a cybersecurity incident?

Discussion

Is there anything suspicious about this email? If yes, what are some details that would increase your suspicion?

What would you do if you were in John's position?

Does your utility/organization have guidance or procedures that cover this type of situation?

Are your employees trained on what to do if they think they have experienced a cybersecurity incident?



Whats happened?

All documents, photos, databases and other **important files encrypted**

How to decrypt files?

The only way to decrypt your files is to receive the **Decryptor**

Are you ready?

We guarantee that you can **recover all your files**. But you have not so enough time.

What guarantees?

If you want to decrypt 1 file for free, write in [Support Chat](#)

Buy Decryptor

Special price now: **25,000 USD / 0.54 BTC**

Current Bitcoin Rate: 1BTC = 45903.42 USD

After **3 days from now** price of this product will increase up to **50,000 USD (price in 1.09 BTC)**

[How buy Decryptor?](#)

Support Chat

x Close

Hello, we're listening, do you have any questions?

Type your message here

John reads the message covering his screen and panics. He opens his “My Documents” folder and notices all his files are still there, but when he tries to open any of them, he is presented with random characters and an error message stating the file is unreadable.

What type of cyber-attack appears to be occurring?

What suggestions do you have for John at this point?

Day 8, 9:52am

As John is contemplating who he should contact, he notices the amount of conversation in the halls is much more than typical and he hears panic in others' voices. Before he can act, he hears a knock at his door and quickly answers.

Standing at his door is his colleague, Christina. Christina notifies John she was delivering a presentation when the deck she was presenting suddenly crashed and would not reopen. She tried to access an older draft version that she remembered was hosted on the town's server, but that too would not open. She then noticed a ransom message had appeared on her screen.

Christina is growing worried because the town's server also holds six years of critical files, financial data, and customer billing information.

Discussion

- At this point, what could (or should) be done to contain the incident?
- Who could John and Christina contact for assistance?
- Is a situation like this included in your Incident Response Plan? If not, make a note to update your plan.

After several more minutes of anxious conversation amongst the staff, the utility manager, Maria, calls everyone into the conference room to discuss the incident. Maria informs the staff it appears they were hit by some type of cyberattack and none of the systems in the office were functioning properly.

- She said she was going to contact their IT vendor, Thomas, as well as activate their Incident Response Plan (IRP) to which they recently added cybersecurity incidents.
- However, upon returning to her office, Maria notices the latest version of the IRP had been stored on the town's files server that was inaccessible. Picking up the phone to call Thomas, she realizes their Voice over IP (VoIP) phone system also appeared to be down. She uses her cell phone to get Thomas on the line.

Why is the IRP unusable? How could this have been prevented?

- Would you be able to access your ERP in a similar situation?

What would you want your staff to know and/or be told in this situation?

Day 8, 11:35am

An hour later, Thomas arrives and begins to evaluate the situation. He confirms the malware seems to have infected all the systems in the utility, including their fileserver and even their VoIP phone system.

Discussing the situation with Maria, he said they luckily had off-line backups of all the files on the file server, but restoring operations on the whole network could take a week or more.

However, before Thomas could even finish briefing Maria, a message appears in the chat box on the ransomware screen: ***“Send payment or we will release your sensitive data to the dark web. Your Customers will not like this. You have 24 hours.”***

Discussion

Does the extortion message from the cyber criminals change your approach to handling the incident? Why or why not?

Should you communicate back with the bad actors? If so, what would you say?

Could this help, or hurt the situation?

Day 8, 11:45am

Understanding the implications of their town's systems being down for over a week and sensitive customer data potentially being leaked, Maria convened a meeting of utility and town leadership for early that afternoon to discuss the incident and the ransomware actor's demands.

Meanwhile, an operator from the town's drinking water treatment facility arrives at the utility office and speaks with Maria and Thomas. He states he has been trying to call them, but their phones appeared to be down.

The operator has observed the SCADA control screens are no longer showing critical process information, including pump and tank status, chemical dosing, and intake control. The chemical feed was frozen at the current feed rates and is no longer responsive.

Discussion

What could be causing the impact to the SCADA system?

What should they do with the SCADA system now that it appears to have been compromised?

How would a SCADA system compromise change your incident response procedures?

Knowing the SCADA system and business system are connected by a flat network, Thomas believes the utility SCADA system problems are due to the ransomware infection as well. Unfortunately, they didn't have any backups of those systems so it could take some time to restore SCADA operations.

Thomas tells the operator that the water treatment process should be disconnected from the business network and operated in a manual mode until they can resolve the problem.

Discussion

Do you agree with Thomas' advice to operate in manual/hand mode?

To what degree could your utility operate manually? For how long? Is this in your Incident Response Plans?

What could have been done to prevent the SCADA system from being compromised?

Maria opens the meeting with the utility and town leadership and begins briefing the situation. Thomas reports after some investigation, they have confirmed the ransomware did spread across connected network from the utility office to the SCADA system.

He also confirmed the ransomware had encrypted critical program files the SCADA system uses to manage water treatment functions and operations are currently impacted.

Maria then reports she had exchanged chat messages with the bad actor and received screenshots confirming they have stolen **174GB** of sensitive data.

They negotiated the ransom demand down to \$20,000 if they pay in the next 12 hours, but they believe the bad actors will act upon their extortion threats if not paid.

Finally, Thomas reported that without the decryption program, it would take up to a week to restore the office systems, and up to a month to restore SCADA operations.

Based on these circumstances, would you suggest they pay the ransom?
Is there anything else that should weigh in the decision?

The leadership team evaluates the potential impact of paying vs not paying the ransom and is torn on how to proceed. While several members are against paying the bad actors their ransom, they have determined it would be far more costly to the utility, and its customers, if they do not pay.

After careful consideration, the leadership reluctantly decided it was best to make a payment to receive the decryption tool, keep out of the media, and protect the utility's data and customers' sensitive data from release.

Payment is made as requested and the bad actors quickly turn over the decryption tool, instructions for its use, and a statement of good faith that the utility's sensitive data being held by the bad actors would be destroyed.

Should you trust the “statement of good faith” from the bad actors that they will destroy the stolen data? Why or why not?

Now that the ransom is paid, what steps should be taken?

With the decryption tool in hand, Thomas and his team work through the night to restore operations to the SCADA network.

However, the process takes far longer than they thought due to some challenges with the decryption tool provided by the cyber criminals, and it still takes them an unexpected **five full days** to restore back to automated operations.

Given the challenges they had with the SCADA network systems, Thomas decides it would be more efficient to restore the town's servers from their backups than to use the decryption tool provided by bad actors.

Discussion

Can this incident be considered resolved now that payment has been made and operations have been restored?

Why or why not?

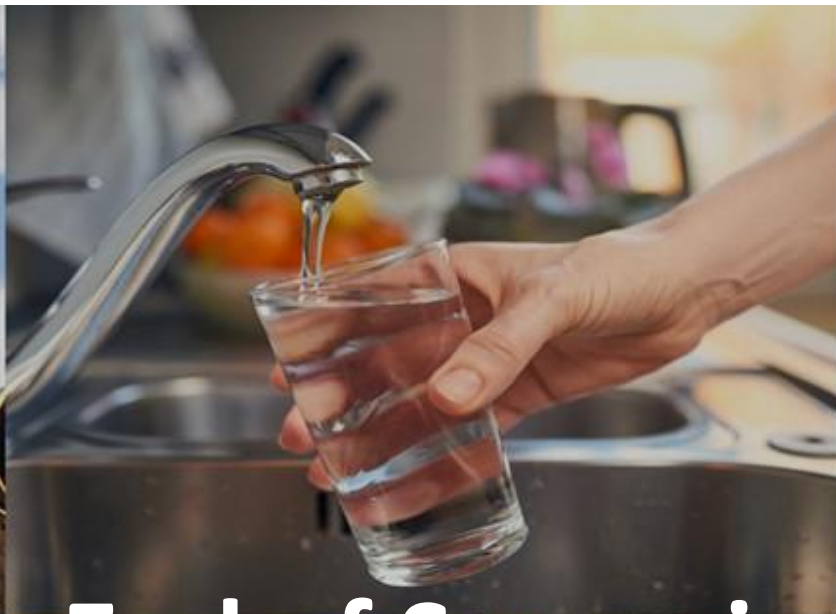
- Does your utility have an estimate on how quickly you could restore operations using your backups?

The Utility Board is meeting at 4:00pm to discuss the incident now that it has been contained. They have asked John, Christina, Maria, and Thomas to provide suggestions on how to raise cybersecurity awareness at the utility and what best practices should be changed moving forward.

What suggestions do you have to raise cybersecurity awareness at their utility?

What cybersecurity best practices should be implemented moving forward?

How can you use an incident such as this to brief management on the need for improved cybersecurity measures at your utility?



End of Scenario





Cyber Threats to Water and Waste Water Systems

- Upset treatment and conveyance processes by opening and closing valves, overriding alarms or disabling pumps or other equipment;
- Deface the utility's website or compromise the email system;
- Steal customers' personal data or credit card information from the utility's billing system; and
- Install malicious programs like ransomware, which can disable business enterprise or process control operations.

Benefits of a Cybersecurity Program

- Ensure the integrity of process control systems –Ensure continuous service
- Protect sensitive utility and customer information
- Reduce legal liabilities if customer or employee personal information is stolen
- Maintain customer confidence

Challenges in establishing cybersecurity programs

- System lacks resources to hire IT specialists to assist
- Utility staff do not not believe or recognize they are at risk for cyber attacks
- Utility staff do not believe they have technical capacity to improve cybersecurity.

Its hopeless and inevitable!

What Can I do ?

Give up ?

Scream and Shout and Run About!

Its hopeless and inevitable!

We Must Practice Safe
Cyber!

Cyber Infrastructure Security Agency (CISA) Recommendations-

- Update to the latest version of the operating system (e.g. Windows 11+).
- Use multiple-factor authentication.
- Use strong passwords to protect Remote Desktop Protocol (RDP) credentials.
- Ensure anti-virus, spam filters, and firewalls are up to date, properly configured and secure.

Cyber Security Recommendations- CISA

- Segregate Networks
- Train users to identify and report attempts at social engineering.
- Identify and suspend access of users exhibiting unusual activity.
- Install backup systems for restoration in the event of an attack.

10 Questions for Cybersecurity (1)

- **Keep an inventory of control system devices and ensure this equipment is not exposed to networks outside the utility?**

Recommendation

- *Never allow any machine on the control network to “talk” directly to a machine on the business network or on the Internet.*

10 Questions for Cybersecurity (2)

- **Segregate networks and apply firewalls?**

Recommendation

- *Classify IT assets, data, and personnel into specific groups, and restrict access to these groups.*

10 Questions for Cybersecurity (3)

- **Use secure remote access methods?**

Recommendation

- *A secure method, like a virtual private network, should be used if remote access is required.*

10 Questions for Cybersecurity (4)

- **Establish roles to control access to different networks and log system users?**

Recommendation

- *Role-based controls will grant or deny access to network resources based on job functions.*

10 Questions for Cybersecurity (5)

- **Require strong passwords and password management practices?**

Recommendation

- *Use strong passwords and have different passwords for different accounts.*

Poll everywhere

Text davidmoney552 to 22333

on the web PollEv.com/davidmoney552

10 Questions for Cybersecurity (6)

- **Stay aware of vulnerabilities and implement patches and updates when needed?**

Recommendation

- *Monitor for and apply IT system patches and updates*

10 Questions for Cybersecurity (7)

- **Enforce policies for the security of mobile devices**

Recommendation

- *Limit the use of mobile devices on your networks and ensure devices are password protected*

10 Questions for Cybersecurity (8)

- **Have an employee cybersecurity training program**

Recommendation

- *All employees should receive regular cybersecurity training*

Poll everywhere

Text davidmoney552 to 22333

on the web PollEv.com/davidmoney552

10 Questions for Cybersecurity (9)

- **Involve utility executives in cybersecurity?**

Recommendation

- Organizational leaders are often unaware of cybersecurity threats and needs

10 Questions for Cybersecurity (10)

- Monitor for network intrusions and have a plan in place to respond?

Recommendation

- *Be capable of detecting a compromise quickly and executing an incident response plan*
- For more information about each of these questions, see WaterISAC 15 Cybersecurity Fundamentals for Water and Wastewater Utilities at <https://www.waterisac.org/fundamentals>

WATER ISAC 15 cybersecurity fundamentals

1. Perform Asset Inventories
2. Assess Risks
3. Minimize Control System Exposure
4. Enforce User Access Controls
5. Safeguard from Unauthorized Physical Access

WATER ISAC 15 cybersecurity fundamentals

6. Install Independent Cyber-Physical Safety Systems
7. Embrace Vulnerability Management
8. Create a Cybersecurity Culture
9. Develop and Enforce Cybersecurity Policies and Procedures
10. Implement Threat Detection and Monitoring

WATER ISAC 15 cybersecurity fundamentals

11. Plan for Incidents, Emergencies, and Disasters
12. Tackle Insider Threats
13. Secure the Supply Chain
14. Address All Smart Devices (IoT, IIoT, Mobile, etc.)
15. Participate in Information Sharing and Collaboration Communities

CISA Top Cyber Actions for Securing a Water System

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.

CISA Top Cyber Actions for Securing a Water System

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.

CISA Top Cyber Actions for Securing a Water System

3. Change Default Passwords Immediately

Require unique, strong, and complex passwords for all water systems, including connected infrastructure.

Change default or insecure passwords and implement multifactor authentication (MFA) where possible

CISA Top Cyber Actions for Securing a Water System

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.

CISA Top Cyber Actions for Securing a Water System

5. Develop and Exercise Cybersecurity Incident Response and Recovery Plans

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.

CISA Top Cyber Actions for Securing a Water System

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.

CISA Top Cyber Actions for Securing a Water System

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

CISA Top Cyber Actions for Securing a Water System

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.

What must utilities do

So I know what I should do

What must I do and when ?

*New requirements for Cyber Security Plans TCA 7-51-2202

- TN office of Comptroller- TN Board of Utility Regulation (TBOUR)
- (a) By July 1, 2023, or within one (1) year after a utility is formed, whichever is later, a utility shall prepare and implement a cyber security plan to provide for the protection of the utility's facilities from unauthorized use, alteration, ransom, or destruction of electronic data.
- (b) A utility shall assess and update the cyber security plan implemented pursuant to this section every two (2) years to address new threats.
 - Comptrollers Office tasked with oversight and verification.
 - Failure to comply will result in referral to WWFB or UMRB (TBOUR)
- During the audit of your utility, you will be required to provide a copy of the cybersecurity plan to your auditor for verification of adoption.

*New requirements for Cyber Security Plans TCA 65-4-127

Tennessee Public Utility Commission

- Requires a cybersecurity plan by July 1, 2023, and updated every two years thereafter
- -TPUC Rules 1220-4-15-.04, Utility Cybersecurity Plans & Reporting
- Requires annual filing that cybersecurity plan is on hand
- Establishes sanctions for failing to comply
- Notification w/in 72 hours of cyber attack unless law enforcement directs otherwise due to on-going investigation

General framework for a Cyber Security Plan

- Identify Cybersecurity roles and responsibility

Identify Assets

- Physical devices and systems
- Software platforms and applications
- Systems and third- party partners-

Detect vulnerabilities

- Vulnerability Auditing
- Scanning
- Security software systems

General framework for a Cyber Security Plan

- Protect/mitigate vulnerabilities
 - Develop policies, SOPs, training etc.
 - Firewalls, access control , alternative storage systems (back up data)
 - Configuration management- separating business and operations systems
- Respond
 - Report to authorities CISA, FBI etc.
 - Implement response plan ,
 - Restore Operations
- Recover
 - Communications
 - Lessons learned
 - Response strategy updates

*EPA requiring states to assess cyber preparedness during Sanitary Surveys

1. March 3, 2023, EPA issues memorandum to states to include Cybersecurity assessments during sanitary surveys.
2. States may allow water utilities to conduct a self-assessment or third-party facilitated assessment prior to the sanitary survey and then review the findings for unaddressed gaps that may represent significant deficiencies.
 - EPA provided cyber assessment tool and 3rd party assistance(HWG)

*EPA requiring states to assess cyber preparedness during Sanitary Surveys

3. July 12, 2023- Judge ordered stay in lawsuit brought by AR, MO, IA .

- TDEC has indicated that it will not implement any process until resolution of litigation.
- Encourages systems to continue to build cyber resilience. It will advocate Options 1A -Self assessment and 1B -Third party assessment

National Security Council Issues letter to Governors

- 03/18/24 letter from WH-NSC to Governors asking states to develop Cyber plans etc.
- https://www.epa.gov/system/files/documents/2024-03/epa-apnsa-letter-to-governors_03182024.pdf
- By June 28, 2024 states are to develop a cybersecurity plan to include how states are working with both drinking water and wastewater systems to determine where they are vulnerable to cyberattacks and what actions they are taking to build in cybersecurity protections.

TDEC Strategyso far

Will rely on the current statutory requirements and offer and assistance in accessing assessment services and plan templates.

Including cyber security awareness as part of the sanitary survey and inspection processes.

Making a requirement for conducting a cyber security assessment to access SRF funding.

EPA issues cybersecurity enforcement alert

June 1, 2024-EPA issues memorandum to states making notification of requirement to address cybersecurity threats.

EPA is increasing inspections and enforcement . Goal of inspecting 50 % of water systems.

EPA reports that's 70% of PWS inspected since September 2023 were in violation of the SDWA to have an EOP. It was required under the 2018 AWIA Risk and Resiliency Assessment. (systems were supposed to include an assessment of cyber vulnerability) and update EOP)

EPA issues cybersecurity enforcement alert

EPA will take enforcement actions against CWS who are found to be cyber vulnerable and or who have not completed the RRA as required.

<https://www.epa.gov/enforcement/enforcement-alert-drinking-water-systems-address-cybersecurity-vulnerabilities>

EPA WCAT Cyber Tool

Since 2023 TAUD staff have been promoting and using the EPA cyber assessment tool.

33 questions - develops an assessment report

TAUD also has developed a cyber security plan template and has example policies that utilities can use.

Tools

WCAT Tool EPA Water Cybersecurity Assessment Tool -taud work shop

Example plan

Cybersecurity Plan Framework

Policy examples cybersecurity policy example1

Cyber Security Policy example II

General framework for a Cyber Security Plan

- Identify Cybersecurity roles and responsibility

Identify Assets

- Physical devices and systems
- Software platforms and applications
- Systems and third- party partners-

Detect vulnerabilities

- Vulnerability Auditing
- Scanning
- Security software systems

General framework for a Cyber Security Plan

- Protect/mitigate vulnerabilities
 - Develop policies, SOPs, training etc.
 - Firewalls, access control , alternative storage systems (back up data)
 - Configuration management- separating business and operations systems
- Respond
 - Report to authorities CISA, FBI etc.
 - Implement response plan ,
 - Restore Operations
- Recover
 - Communications
 - Lessons learned
 - Response strategy updates

Funding Opportunities

Nations Infrastructure Bill 2021 signed into law 11/15/21

- \$55 billion for water infrastructure replacement
- \$50 Billion for System resiliency to address cyber security and natural disasters.

Funding will flow through TN SRF program.

The Cyber Security Evaluation Tool (CSET)

- The Cyber Security Evaluation Tool (CSET) provides a systematic, disciplined, and repeatable approach for evaluating an organization's security posture.
- CSET is a desktop software tool that guides asset owners and operators through a step-by-step process to evaluate industrial control system (ICS) and information technology (IT) network security practices.
- Users can evaluate their own cybersecurity stance using many recognized government and industry standards and recommendations.



CISA Known Exploited Vulnerabilities Catalog (KEV)



CYBERSECURITY
& INFRASTRUCTURE
SECURITY AGENCY



Report Cyber Issue

Subscribe to Alerts



CYBERSECURITY



INFRASTRUCTURE
SECURITY



EMERGENCY
COMMUNICATIONS



NATIONAL RISK
MANAGEMENT



ABOUT
CISA



MEDIA

KNOWN EXPLOITED VULNERABILITIES CATALOG

[Download CSV version](#)

[Download JSON version](#)

[Download JSON schema](#)

[Subscribe to the Known Exploited Vulnerabilities Catalog Update Bulletin](#)

[Back to previous page for background on known exploited vulnerabilities](#)

Show entries

Search:

CVE	Vendor/Project	Product	Vulnerability Name	Date Added to Catalog	Short Description	Action	Due Date	Notes
-----	----------------	---------	--------------------	-----------------------	-------------------	--------	----------	-------

CVE-2021-27104

Accellion FTA

Accellion FTA9_12_370 and earlier is affected by

Ask AI Assistant

Short on time? Ask for a quick summary



Cyber Security/ Resilience Resource Opportunities

- EPA Cybersecurity Best Practices for the Water Sector. Includes cybersecurity Incident Action Checklist and training opportunities. . <https://www.epa.gov/waterriskassessment/epa-cybersecurity-best-practices-water-sector>
- EPA is making [Free Cybersecurity Assessment and Technical Assistance](#) available to drinking water and wastewater utilities. This is a great opportunity for help with an assessment and the development of a cyber action plan.
- <https://www.epa.gov/waterriskassessment/epa-cybersecurity-water-sector#TA>
- Cyber & Infrastructure Security Agency (CISA) -Free cyber hygiene services -vulnerability scanning.
 - Provides periodic scans of your systems and weekly reports of the scans. <https://www.cisa.gov/cyber-hygiene-services>
- <https://www.cisa.gov/uscert/resources>
- <https://www.awwa.org/Resources-Tools/Resource-Topics/Risk-Resilience/Cybersecurity-Guidance>
- <https://www.awwa.org/Resources-Tools/Resource-Topics/Risk-Resilience/Cybersecurity-Guidance>
- <https://www.waterisac.org/system/files/articles/15%20Cybersecurity%20Fundamentals%20%28WaterISAC%29.pdf>
- https://www.epa.gov/sites/default/files/2017-11/documents/171013-incidentactionchecklist-cybersecurity_form_508c.pdf



Additional Water and Wastewater Systems Sector Guidance Resources

- [Cybersecurity Fundamentals for Water and Wastewater Utilities](#) | [WaterISAC](#)
- [Top Cyber Actions for Securing Water Systems](#) | [CISA](#)
- [Water and Wastewater Sector - Incident Response Guide](#) | [CISA](#)
- [CISA's Free Cyber Vulnerability Scanning for Water Utilities](#) | [CISA](#)
- [Water and Wastewater Cybersecurity](#) | [CISA](#)
- [Exploitation of Unitronics PLCs used in Water and Wastewater Systems](#)
- [Water and Wastewater Sector - Incident Response Guide](#) (CISA)

Incident Reporting

WaterISAC encourages any members who have experienced malicious or suspicious activity to email analyst@waterisac.org, call 866-H2O-ISAC, or use the confidential [online incident reporting form](#).



Poll everywhere

Text davidmoney552 to 22333

on the web PollEv.com/davidmoney552

Q6

Q6

Contact Information

David Money

Tennessee Association of Utility Districts

931-477-0963

DavidMoney@taud.org