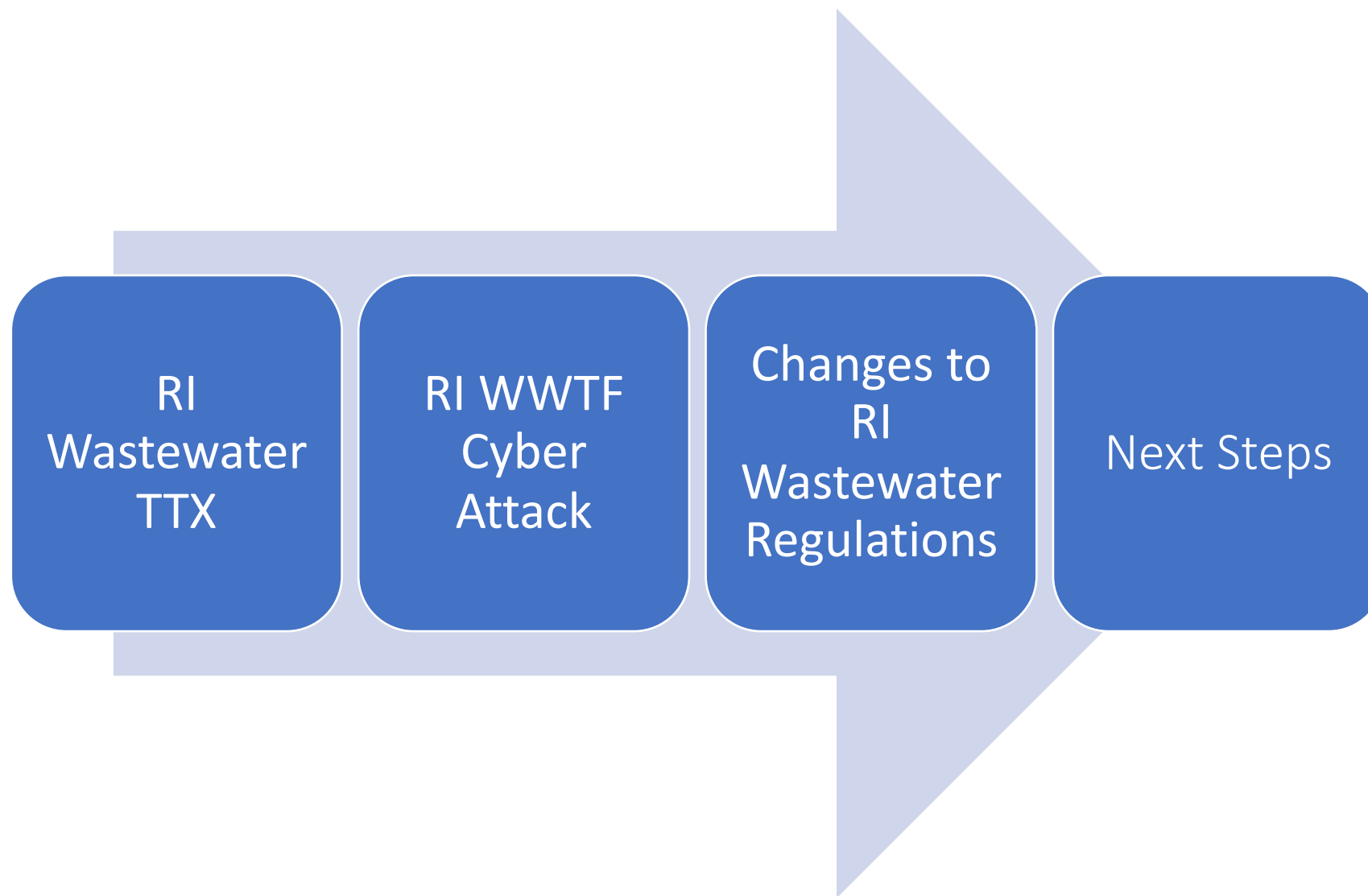


Protecting the Unseen Assets: The Addition of Cybersecurity to Rhode Island State Regulations

Jack Segal, EIT
Rhode Island Department of
Environmental Management



*How many ransomware attacks
occur every day?*

7,855 Ransomware Attacks Occur Nationwide every day

That's one every 11 seconds

Source: 2022 CISA Chemical Supply Summit





No regulations

No standardized
cybersecurity
baseline

Variable
Cybersecurity at
WWTFs

- Cybersecurity and Infrastructure Security Agency (CISA)
- Water Information and Sharing Analysis Center (WaterISAC)
- Two Objectives
 1. Improve stakeholder knowledge
 2. Identify areas of improvement



**CYBERSECURITY &
INFRASTRUCTURE
SECURITY AGENCY**



- Improving Stakeholder Knowledge
 - Who is affected?
 - Who/What is the threat(s)?
 - What the magnitude of the threat?
 - Response to a cyberattack/compromise
 - Recovery from a cyberattack

- Identify Areas for Improvement

- Requesting/Sharing emergency cyber resources
- Internal/external communications
- Best practices for a cyber incident
- Information sharing/coordination with internal and external partners
- Identify triggers, escalation criteria, and notification thresholds



*National Institute of Standards and
Technology (NIST) Cybersecurity
Framework*

- Tabletop Exercise Feedback
 - *“A list of contacts of all the Rhode Island regulatory and law enforcement contacts to add to my “Incident Response Procedures”*
 - *“Send out an email to superintendents if any potential or known cyber threats occur”*
 - *“Encourage facilities to share known threats with [other] facilities”*
 - *“We’ll review our crisis operation plan in hopes of improving it”*

Wastewater Sector Cybersecurity (September 2022)



RHODE ISLAND
DEPARTMENT OF ENVIRONMENTAL MANAGEMENT
OFFICE OF WATER RESOURCES
235 Promenade Street, Providence, Rhode Island 02908



September x, 2022

Municipal Contact
Address 1
Address 2
City, State, Zip

RE: Wastewater Sector Cybersecurity

At a September 9, 2022 meeting of Rhode Island wastewater treatment managers, representatives of the Office of Water Resources (OWR) were joined by R. Michael Tetreault, Cybersecurity Advisor for Rhode Island from the U.S. Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (DHS-CISA), for an update on wastewater cybersecurity efforts. As you know, evolving international matters have heightened concerns of cyber-attacks—concerns that have been realized with the July ransomware compromise of a wastewater utility in Rhode Island.

Below are three items noted by OWR and DHS-CISA at the September 9 meeting:

1. The findings of a DHS-CISA tabletop training for the Rhode Island wastewater sector have been forward to OWR for its use to better understand the state of cybersecurity throughout the sector. Those findings are provided in the attached.
2. Over the next few months, OWR will use these findings to incorporate cybersecurity in its inspections of and expectations for the wastewater collection and treatment sector.
3. To assist communities/facilities in better protecting their wastewater infrastructure and business operations, all owners and operators of said wastewater systems should avail themselves to the information, technical assistance reviews, and other resources provided free of charge by DHS-CISA. These resources also include evaluations for improvements of physical security. More information can be found at <https://www.cisa.gov/>. To arrange site/community-specific reviews, contact DHS-CISA's Mr. Tetreault directly at roland.tetreault@cisa.dhs.gov.

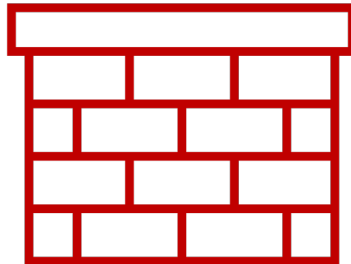
Please note that when considering enforcement actions for Rhode Island Discharge Elimination System permit violations, OWR will consider the extent to which communities/facilities undertook efforts to protect system cyber integrity, as well as to respond to and recover from cybersecurity compromises.

Should you or your staff have any questions regarding OWR's cybersecurity efforts, please contact Mr. William Patenaude at bill.patenaude@dem.ri.gov.

Sincerely,

Firewall

- Controls network traffic based on pre-defined rules
- *Like the security checkpoint at airports*

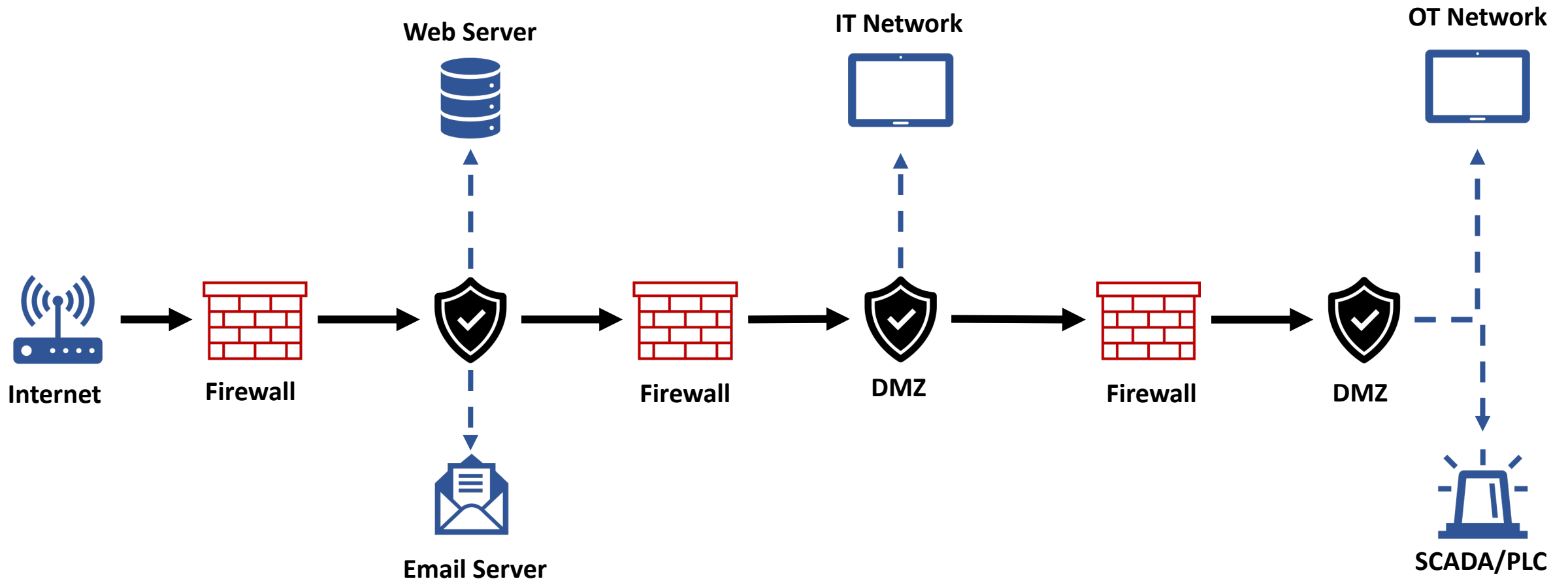


Demilitarized Zone

- Protects public-facing services
- Segments the network (trusted, DMZ, untrusted)
- *Like security guards patrolling airports*



Network Segmentation & Training



- Develop and implement an integrated data recovery management plan that incorporates 3-2-1 backup strategy and test backups
- Implement scans of backs to ensure data integrity

3 copies of Any Important File



2 Types of Locations/Media




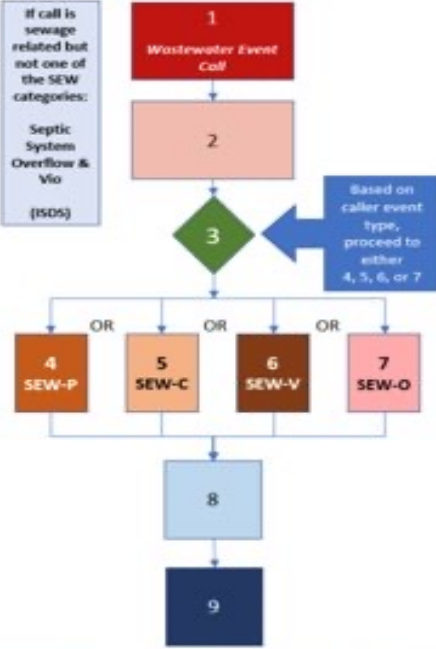


1 Copy Kept Offline/Off Network



Tabletop Exercise Key Takeaways (June 2022)



- Exercise and update crisis communications plan at least annually
- Develop “scripts” for coordinating with IT, legal, public affairs, and regulatory personnel

Seq. No	 Process Name: WWTF Call To DEM Law Enforcement FOR USE DURING NON-BUSINESS HOURS	Standard Work Instruction Sheet			
		SWIS #	DEM-DLE-001	REV # 3	0
ELEMENTS OF OPERATION		JOB LAYOUT (details)			
1	WWTF: CALL DEM DISPATCH 401-222-3070	 <p>Example of Plant Location (#4) </p> <p>Example of Collection Location (#5) </p>			
2	WWTF: When Dispatcher answers, inform dispatcher "This is a Wastewater Event Call from (Name of Facility/Community). My name is (state your full name) and the contact number is (provide a phone number that can be called if additional information is needed). The event is a (provide one of the call category titles in boxes 4, 5, or 6.)"				
3	DISPATCHER: Ask the numbered questions in the appropriate call-reason box. Note: Caller may not have all information, in which case record the information as "Unknown." OTHER SEWERAGE CALLS USE SEPTIC SYSTEM OVERFLOW & VIO (Code: ISOS)				
4	FOR A SEW. PLANT DISCHARGE: Dispatcher questions: 1. "What is the nature of the process or equipment failure?" 2. "What is the approximate start time and end time, if known?" 3. "Are you reporting known permit violations, if so, what are they?" 4. "What is the approximate flow volume of any partially or untreated discharge?" (End questions: Go to Box 8)				
5	FOR A SEW. COLLECTION SY. DISCHARGE: Dispatcher questions: 1. "What is the location of the event?" 2. "What is the approximate start time and end time, if known?" 3. "What water bodies, if any, are impacted?" 4. "What is the estimated volume or flow rate, if known?" (End questions: Go to Box 8)				
6	FOR A SEW. PLANT PERMIT VIO: Dispatcher questions: 1. "What is the parameter violated?" 2. "What is the approximate numerical value and unit?" 3. "Is this violation the result of a plant failure?" 4. "If yes, please briefly explain." (End questions: Go to Box 8)				
7	IF UNSURE OF CATEGORY, USE: SEW. DISCHARGE OTHER: Dispatcher questions: 1. "Nature of violation or issue." 2. "What water bodies, if any, are impacted?" 3. "What is the estimated volume or flow rate?"				
8	WWTF: Ask for the name of the dispatcher.				
9	DLE/WWTF: End call.				
REQUIRED SKILLS		Effective Date:	TBD	Revisions Highlighted in Yellow	
		Author:	Bill Patenaude		
		Supervisor Approval:	Steve Criscione		
		Lean Team Approval:	Lou Maccarone		
				Page 1 of 1	

2022 Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA)

Report@cisa.gov



Payment will be raised on

5/15/2017 16:50:06

Time Left

02:23:34:22

Your files will be lost on

5/19/2017 16:50:06

Time Left

06:23:34:22

[About bitcoin](#)

[How to buy bitcoins?](#)

[Contact Us](#)

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday.



Send \$300 worth of bitcoin to this address:

115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn

Copy

Check Payment

Decrypt

Rhode Island WWTF Cyber Compromise (July 2022)



- WWTF targeted in a cyberattack
- Victim of Ransomware

A screenshot of a ransomware payment screen. The background is dark red. At the top left, there is a white padlock icon. The main text is in white and yellow. The screen is titled "Ooops, your files have been encrypted!". It contains sections for "What Happened to My Computer?", "Can I Recover My Files?", and "How Do I Pay?". There are two countdown timers: "Payment will be raised on 5/15/2017 16:50:06" with a time left of "02:23:34:22", and "Your files will be lost on 5/19/2017 16:50:06" with a time left of "05:23:34:22". At the bottom, there is a Bitcoin logo, a text box with the address "115p7UMMngoj1pMvkhHijcRdfJNXj6LrLn", and buttons for "Check Payment" and "Decrypt".

Ooops, your files have been encrypted! English

What Happened to My Computer?
Your important files are encrypted. Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time. You can decrypt some of your files for free. Try now by clicking <Decrypt>. But if you want to decrypt all your files, you need to pay. You only have 3 days to submit the payment. After that the price will be doubled. Also, if you don't pay in 7 days, you won't be able to recover your files forever. We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>. Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>. And send the correct amount to the address specified in this window. After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT From Monday to Friday

Payment will be raised on
5/15/2017 16:50:06
Time Left
02:23:34:22

Your files will be lost on
5/19/2017 16:50:06
Time Left
05:23:34:22

[About bitcoin](#)
[How to buy bitcoins?](#)
[Contact Us](#)

Send \$300 worth of bitcoin to this address:
 **115p7UMMngoj1pMvkhHijcRdfJNXj6LrLn** Copy

Check Payment **Decrypt**

Rhode Island WWTF Cyber Compromise (July 2022)



- WWTF targeted in a cyberattack
- Victim of Ransomware
- Backups corrupted
- Did not compromise wastewater treatment

A screenshot of a ransomware payment screen with a dark red background. At the top left is a white padlock icon. The main text reads "Ooops, your files have been encrypted!" in white. Below this are two sections with yellow text: "Payment will be raised on 5/15/2017 16:50:06" and "Your files will be lost on 5/19/2017 16:50:06", each followed by a "Time Left" counter showing "02:23:34:22" and "06:23:34:22" respectively. The right side contains a white text area with sections: "What Happened to My Computer?", "Can I Recover My Files?", and "How Do I Pay?". At the bottom right, there is a Bitcoin logo, the text "Send \$300 worth of bitcoin to this address:", and a Bitcoin address "115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn" with a "Copy" button. At the bottom are "Check Payment" and "Decrypt" buttons. Links for "About bitcoin", "How to buy bitcoins?", and "Contact Us" are at the bottom left.

Rhode Island WWTF Cyber Compromise (July 2022)



- WWTF targeted in a cyberattack
- Victim of Ransomware
- Did **not** compromise wastewater treatment
- Backups corrupted
- Costs
 - Facility paid **\$250,000** for ransom

A screenshot of a ransomware payment screen with a dark red background. At the top left is a white padlock icon. The main heading reads "Ooops, your files have been encrypted!". Below this are two sections: "Payment will be raised on" with a date of 5/15/2017 16:50:06 and a "Time Left" of 02:23:34:22; and "Your files will be lost on" with a date of 5/19/2017 16:50:06 and a "Time Left" of 06:23:34:22. The central text explains the encryption and offers a way to recover files by paying. A Bitcoin logo and "ACCEPTED HERE" text are shown next to a Bitcoin address: 115p7UMMngo1pMvKpHijcRdfJNXj6LrLn. At the bottom are "Check Payment" and "Decrypt" buttons. A language dropdown menu is set to "English".

Rhode Island WWTF Cyber Compromise (July 2022)



- WWTF targeted in a cyberattack
- Victim of Ransomware
- Did **not** compromise wastewater treatment
- Backups corrupted
- Costs
 - Facility paid **\$250,000** for ransom
 - More administrative and IT costs
 - Hardware costs
 - Time spent
 - Credit monitoring for current and past employees

A screenshot of a ransomware payment screen. The background is dark red. At the top left is a white padlock icon. The main text is white and yellow. It says "Ooops, your files have been encrypted!" in white. Below that, it asks "What Happened to My Computer?" and "Can I Recover My Files?". There are two countdown timers: "Payment will be raised on 5/15/2017 16:50:06" and "Your files will be lost on 5/19/2017 16:50:06". At the bottom, it says "How Do I Pay?" and provides a Bitcoin address: "115p7UMMngo1pMvKpHijcRdfJNXj6LrLn". There are buttons for "Check Payment" and "Decrypt".

- “Asset”
- “Asset Management”
- “Cyber Compromise”
- “Cyber Resilience Review”
- “Cybersecurity”
- “National Preparedness Goals”
 - Prevention, Protection, Mitigation, Response, and Recovery
- “Resilience”
- “Risk and Resilience Coordinator”
 - Aim to meet the National Preparedness Goals
 - Administer training and organize resources



FEMA

- 4.5 Operation and Maintenance Plan Requirements
- Descriptions of provisions to ensure security and resilience
 - Documentation of plans for threat identification, prevention, protection, mitigation, response, and recovery.
 - Emergency procedures and reporting requirements
 - Power outages
 - Natural disasters
 - Cyber Compromises
 - SSOs



#StopRansomware Guide

- 4.6 Procedures for the Evaluation of a Plan
 - NIST Cybersecurity Framework listed as a guidance document
- 4.10 Records of Operation
 - DEM can require documentation of any equipment or electronic system failure or compromise
 - Provide other information relating to the operation, maintenance, or compromise of a Wastewater Treatment Facility

Next Steps



- Meet with all Municipal WWTFs and discuss the potential changes
- Proposed WWTF Regulation Changes review and submittal
- Proposed/Potential Permit Changes
- Collaboration with CISA and RIEMA
- Communication with WWTF about Cyber Grants and CWSRF
- Update Regulatory Expectations and Guidance

Acknowledgements



Mike Ietreat, CISA
Cybersecurity Advisor for RI



Matt Puglia, RI DEM
Operations & Maintenance Program



Christine Willette, RI EMA
CIKR Coordinator

Joseph Haberek, RI DEM
Administrator for Surface Water
Protection

Bill Patenaude

Questions