ORWARN
Oregon Water/Wastewater Agency Response Network

Oregon Water/Wastewater Agency Response Network (ORWARN) Cyber Tabletop Exercise

July 17, 2024

Exercise Purpose:

Examine the information sharing, coordination, and incident response capabilities of ORWARN stakeholders in response to a significant cyber incident affecting water/wastewater systems.

Objectives:

1. Discuss utility stakeholders' information sharing processes with internal and external stakeholders.
2. Explore utility member's ability to identify and respond to a cybersecurity incident.
3. Examine internal and external communications protocols and capabilities of utility stakeholders during a cyber incident.
4. Identify utility stakeholders' processes for requesting additional resources once their resources are exhausted.

Module 1

Ice Breaker

1. What is the greatest cybersecurity threat to your organization?

Day 1

The Cybersecurity & Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI) issue a joint alert regarding a rise in cyberattacks targeting water and wastewater institutions. The alert describes the tactics, techniques, and procedures used by cyber criminals, including phishing emails, ransomware, distributed denial of service attacks, and data exfiltration from water and wastewater agencies. These attacks are expected to continue throughout the year.

Discussion Questions

2. What cybersecurity threat information does your organization receive?
   a. What actions would be taken based on this information?

Day 2

Employees receive an urgent email that appears to be from IT. It notifies them of an immediate change to password requirements due to the rise in cyberattacks targeting water and wastewater organizations. The email states that employees who fail to update their passwords will lose access to the network. Those who click on the link are taken to a page that looks like your organization's website and are prompted to log in using their credentials.

Discussion Questions

3. How would you describe your organization's cybersecurity posture?
   a. How frequently are users required to change their passwords?
   b. Does your organization utilize multi-factor authentication (e.g., something you know, something you have, something you are) to mitigate the potential effects of phishing?
4. How do users report suspicious emails?
   a. What procedures or plans would be followed once a suspicious email has been reported?

Day 4

A long-time employee is reported by a colleague as being seen entering and exiting server rooms at strange times during the workday with an unknown cable. When approached by a manager the employee explains they were completing routine checks on systems and there is nothing to worry about. Satisfied, the manager drops the issue.

Discussion Questions

5. What processes do you use to assess cyber risks within your network?
6. Describe your organization's cybersecurity training program.
   a. How frequently do employees receive cybersecurity training?
   b. What are your training requirements for third-party vendors who access your network/systems?

Day 5

Employees begin calling IT complaining that their computers are running a bit slow, and some company applications, websites, and SharePoint are taking a while to open.

Day 8

Employees arrive to work on a Monday morning and find they are unable to access files, the intranet, Office 365, and network drives. Restarts do not solve the problem. Calls begin coming into the IT Helpdesk.

Discussion Question

7. Describe the actions you would take to address the computer latency and the inability to access required files/drives.

Module 2

Day 9 – Morning

The utility manager informs staff that none of the networks/systems are functioning properly.

The Voice over IP (VoIP) phone system is also inoperable.

Day 9 - Evening

An operator at the water-treatment plant observes that SCADA control screens are no longer showing critical process information, including pump and tank status, chemical dosing, and intake control.

Discussion Question

1. What are your priorities based on the events so far?

Day 10

Employees try to log into your organization's system, and see the following message displayed on their devices:

"We own your data. For $500,000.00 in Bitcoin, your files will be returned. Submit payment by clicking the link below, or everything will be posted for sale to the highest bidder. Don't believe us? We will publish your data every 24 hours.

Discussion Questions

2. Describe the decision-making process following a ransomware incident.
   a. How are your cyber insurance provider or third-party vendors involved in your procedures?
3. How does the release of sensitive information or Personally Identifiable Information (PII) impact incident response and recovery actions?
4. What are the potential legal and reputational ramifications?

Day 11

Your IT vendor reports they have confirmed the ransomware spread across the flat network from the business network to the SCADA system. The ransomware attack encrypted critical program files the SCADA system uses to manage water treatment functions, impacting operations.

Discussion Questions

5. What actions would be taken based on your organization's incident response plan?
   a. How long can you operate using manual procedures?
   b. What backups do you have to facilitate system recovery and how often are they tested?
   c. How long would it take to recover and restore impacted systems?
6. What notifications are you making?
   a. What information is being shared internally (e.g., staff, leadership)?
   b. What information is being shared externally (e.g., public, law enforcement, state agencies)?

Module 3

Day 12

The attackers published a sample of your organization's data on a hacker forum. They claim they will release more data every 4 hours unless an additional payment of $50,000 in bitcoin is received.

Discussion Questions

1. Discuss your response to the data exfiltration.
    a. How do you verify the data is from your organization's employees?

Day 13

A social media post begins trending with #InHotWater and a screenshot of the hacker forum. The screenshot includes customer names, telephone numbers, customer addresses, and payment information. Customers angrily call your organization for answers about what is being done to protect their personal information.

Discussion Questions

2. What communications plan does your organization's public information office have for responding to cyber incidents?
    a. How will you ensure continuity of the information being shared with leadership, customers, and employees?

Day 14 - morning

Customers are calling about odor and taste concerns in their water. They begin posting pictures of their tap water on social media with #StinkyWater, to let individuals know about the poor water quality provided by your organization.

Discussion Questions

3. How sufficient are your organization's current internal resources for responding to cyber incidents in this scenario?
    a. What additional resources would you need and what is the process for requesting them?
4. How does your organization ensure water quality?
    a. How often is water testing conducted?

Day 14 - afternoon

Your local news outlet calls your organization's headquarters asking for comments on the ransomware incident and impacts on the public. Several customers have been interviewed by the news outlet and express concerns for the safety of drinking water.

Discussion Questions

5. How would your organization address these incidents with the local media?
6. What steps would your organization take to regain public trust?
7. What are your processes for determining when an incident is resolved?
8. Describe your lessons learned/corrective action process.
    a. How are recommendations implemented and tested?

Please complete the feedback form using the QR code or entering the following link into your phone, tablet, or laptop browser https://forms.office.com/g/r5KZjCBm9N

For more information about the National Cyber Exercise Program, please contact: cisa.exercises@cisa.dhs.gov