[Enter Client Name]

CISA Tabletop Exercise Package – Water Systems

<Exercise Date>

U.S. Department of Homeland Security
Cybersecurity and Infrastructure Security Agency

Table of Contents

DISCLAIMER: This report is provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information within. DHS does not endorse any commercial product or service referenced in this advisory or otherwise. This document is distributed as TLP:WHITE: Disclosure is not limited. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction. Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to. For more information on the Traffic Light Protocol, see https://www.us-cert.gov/tlp.

Handling Instructions

Delete instructions that are not applicable.

TLP: AMBER [Delete this qualifier]

The title of this document is <Exercise Title> Situation Manual. This document is unclassified <if applicable> and designated as *"Traffic Light Protocol (TLP):AMBER"*<if applicable> This designation is used when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved. Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. **Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.**

This document should be disseminated to applicable partners and stakeholders on a need-to-know basis pursuant to TLP:AMBER and <exercise sponsor name or other authority> guidelines due to the sensitivity of the information contained herein.

For questions about this event or recommendations for improvement contact: [Name], [Title] at ###-###-#### or [email address] <of sponsoring organization>.

TLP: GREEN [Delete this qualifier]

The title of this document is <Exercise Title> Situation Manual. This document is unclassified <if applicable> and designated as *"Traffic Light Protocol (TLP):GREEN"*: Limited disclosure, restricted to the community. Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector. Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. **TLP:GREEN information may not be released outside of the community.**

This document should be disseminated to applicable partners and stakeholders on a need-to-know basis pursuant to TLP:GREEN and <exercise sponsor name or other authority> guidelines due to the sensitivity of the information contained herein.

For questions about this event or recommendations for improvement contact: [Name], [Title] at ###-###-#### or [email address] <of sponsoring organization>.

TLP: RED [Delete this qualifier]

The title of this document is <Exercise Title> Situation Manual. This document is unclassified <if applicable> and designated as *"Traffic Light Protocol (TLP):RED"*: Not for disclosure, restricted to participants only.

Sources may use TLP:RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused. Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, **TLP:RED should be exchanged verbally or in person.**

This document should be disseminated to applicable partners and stakeholders on a strict need-to-know basis pursuant to TLP:RED and <exercise sponsor name or other authority> guidelines due to the extreme sensitivity of the information contained herein.

For questions about this event or recommendations for improvement contact: [Name], [Title] at ###-###-#### or [email address] <of sponsoring organization>.

TLP: WHITE [Delete this qualifier]

The title of this document is <Exercise Title> Situation Manual. This document is unclassified <if applicable> and designated as "*Traffic Light Protocol (TLP):WHITE*": Disclosure is not limited. Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. **Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.**

This document may be disseminated publicly pursuant to TLP:WHITE and <exercise sponsor name or other authority> guidelines.

For questions about this event or recommendations for improvement contact: [Name], [Title] at ###-###-#### or [email address] <of sponsoring organization>.

Exercise Overview

<table>
<tr><th>Exercise Name</th><th colspan="2">Exercise Title</th></tr>
<tr><td>Exercise Date, Time, and Location</td><td colspan="2">Exercise Date
Time (e.g. 9:00 a.m. – 12:00 p.m.)
Exercise Location</td></tr>
<tr><td rowspan="10">Exercise Schedule</td><th>Time</th><th>Activity</th></tr>
<tr><td>Time</td><td>Activity</td></tr>
<tr><td>Time</td><td>Activity</td></tr>
<tr><td>Time</td><td>Activity</td></tr>
<tr><td>Time</td><td>Activity</td></tr>
<tr><td>Time</td><td>Activity</td></tr>
<tr><td>Time</td><td>Activity</td></tr>
<tr><td>Time</td><td>Activity</td></tr>
<tr><td>Time</td><td>Activity</td></tr>
<tr><td>Time</td><td>Activity</td></tr>
<tr><td>Scope</td><td colspan="2">X hour facilitated, discussion-based tabletop exercise</td></tr>
<tr><td>Purpose</td><td colspan="2">Examine the readiness of water treatment plants to detect and respond to cyber incidents.</td></tr>
<tr><td>INSERT: <NIST, FEMA, or Mission Capabilities></td><td colspan="2">For example, areas such as Identify, Protect, Respond, etc.</td></tr>
<tr><td>Objectives</td><td colspan="2">1. Evaluate plans, procedures, roles, responsibilities, and capabilities of the information technology (IT) and operational technology (OT) personnel when responding to potential cyber threats.
2. Evaluate the role of external entities and officials (e.g., local, state, and federal law enforcement) during a cyber incident.
3. Discuss internal coordination efforts required to respond to a cyber incident.
4. Discuss external coordination between the [Water System] and other entities to develop and disseminate information, alerts, and warnings to the public in response to a cyber incident.</td></tr>
<tr><td>Threat or Hazard</td><td colspan="2">Cyber</td></tr>
<tr><td>Scenario</td><td colspan="2">A threat actor targets valves, pumps, and fail-safe protection systems, and subsequently starts tarnishing their public reputation via social media.</td></tr>
<tr><td>Sponsor</td><td colspan="2">Exercise Sponsor</td></tr>
<tr><td>Participating Organizations</td><td colspan="2">Overview of organizations participating in the exercise (e.g. federal, state, local, private sector, etc.).</td></tr>
</table>

Exercise Name	Exercise Title	
Points of Contact (POCs)	Insert Organization POC(s) Contact info	DHS CISA Exercises CEP@hq.dhs.gov CISAServiceDesk@us-cert.gov

General Information

Participant Roles and Responsibilities

The term *participant* encompasses many groups of people, not just those playing in the exercise. Groups of participants involved in the exercise, and their respective roles and responsibilities, are as follows:

Players have an active role in discussing or performing their regular roles and responsibilities during the exercise. Players discuss or initiate actions in response to the simulated emergency.
Observers do not directly participate in the exercise. However, they may support the development of player responses to the situation during the discussion by asking relevant questions or providing subject matter expertise.
Facilitators provide situation updates and moderate discussions. They also provide additional information or resolve questions as required. Key Exercise Planning Team members may also assist with facilitation as subject matter experts during the exercise.
Note-takers are assigned to observe and document exercise activities. Their primary role is to document player discussions, including how and if those discussions conform to plans, policies, and procedures.

Exercise Structure

This exercise will be a multimedia, facilitated exercise. Players will participate in the following:

- Cyber threat briefing (if desired)
- Scenario modules:
  - **Module 1:** Identification & Protection
  - **Module 2:** Detection & Response
  - **Module 3**: Recovery
- Hotwash

Exercise Guidelines

- This exercise will be held in an open, no-fault environment. Varying viewpoints are expected.
- Respond to the scenario using your knowledge of existing plans and capabilities, and insights derived from your training and experience.
- Decisions are not precedent setting and may not reflect your organization’s final position on a given issue. This exercise is an opportunity to discuss and present multiple options and possible solutions and/or suggested actions to resolve or mitigate a problem.
- There is no hidden agenda, and there are no trick questions. The resources and written materials provided are the basis for discussion.
- The scenario has been developed in collaboration with subject matter experts and exercise planners from your organization.
- In any exercise, assumptions and artificialities are necessary to complete play in the time allotted, to achieve training objectives, and/or account for logistical limitations. Please do not allow these considerations to negatively impact your participation in the exercise.

Exercise Hotwash and Evaluation

The facilitator will lead a hotwash with participants at the end of the exercise to address any ideas or issues that emerge from the exercise discussions.

Module 1: Identification & Protection

Day 1, 8:00 a.m.

The Cybersecurity and Infrastructure Security Agency (CISA) and the Water Information Sharing and Analysis Center (WaterISAC) jointly release a security alert regarding two vulnerabilities found in a popular remote desktop software used by water treatment facilities. The alert states that the vulnerabilities can be exploited to remotely execute code on targeted remote desktop servers prior to authentication. CISA and WaterISAC advise all water systems to utilize up-to-date software and promptly apply corresponding critical patches.

Day 7, 9:00 a.m.

An employee notices code running within a command prompt on a control console. This workstation is responsible for controlling pumps and configuring water flow. The command prompt then quickly terminates and closes. The employee notifies the Information Technology (IT) department.

Discussion Questions

Discussion questions included in each module may be modified as desired. Additional questions can be found in Appendix A.

1. What sources of cybersecurity threat intelligence does your organization utilize?
2. How does your organization process cybersecurity alert information?
3. Describe the procedure regarding integration of new components and connections (e.g., equipment, devices, software) to your network.
4. Describe the process for ensuring patches are up to date.
5. Describe the steps taken once equipment running on your networks is operating beyond the end of life date and is no longer supported for patching/updates.
6. How do you monitor your network technology or system to view and flag suspicious code executions, application processes, and activities on internal machines?
   a. What is the process once an alert about suspicious activity is received from network monitoring?
7. How do you handle user account creation?
   a. How do you control who has access to specific accounts or systems?
8. What is the process for employees to report something suspicious or unusual on one of your networks?
   a. What happens after an employee reports something suspicious or unusual on one of your networks?

Day 10, 10:00 a.m.

Several [Water System] employees receive an official-looking email from the Human Resources (HR) Department with the subject “Mandatory Security Training: Complete by COB.” Employees are instructed to click an embedded link in the email. Upon clicking, they are returned to a “404 error: File not found” page. A few employees contact HR and say they’re unable to access the link. Others decide to try later.

Day 14, 11:00 a.m.

Some employees notice that a small remote desktop program window launches on their desktop and then disappears immediately. Most employees dismiss it as a glitch, but a few employees contact their supervisors and IT security to report the problem.

Discussion Questions

9. What training do your employees receive on how to recognize and report a suspicious email?

10. How would your HR and IT personnel respond to suspected phishing emails?

11. What actions are taken if employees click on a malicious link in a phishing email?

12. What kind of cybersecurity training do you provide to employees?

    a. Are there additional training requirements for IT managers, operational technology (OT) managers/staff, system and network administrators, vendors, or other personnel with access to system-level software?

13. What policies and/or procedures are in place to address unusual issues on individual workstations?

    a. What actions would you take to address it?

    b. What processes would you use to analyze the problem?

    c. Who can declare an emergency and what are the policies/procedures? Are these well-known?

Day 26

Several distribution valves around different areas of the [Water System] facility open and close at unscheduled, random times. Control system operators note the occurrence and determine it to be a singular malfunction in otherwise normal operations.

Discussion Questions

14. Is the malfunction an OT issue or a cyber/IT issue?

    a. How do you distinguish between a mechanical malfunction and a cyber-related error?

    b. How would you respond to a cyber intrusion?

15. How do your OT and IT teams interact?

    a. Describe the coordinating procedures between the two groups in response to an incident or event that involves both aspects.

16. How do you protect your OT networks?

    a. Are your OT systems segmented?[1]

[1] Network segmentation is defined as "an architectural approach that divides a network into multiple segments or subnets, each acting as its own small network," which allows network administrators to have greater control over access to each segmented network. Visit https://www.paloaltonetworks.com/cyberpedia/what-is-network-segmentation for more information.

i. If so, how are they segmented (e.g., VLAN, IP, IP networks, subnets, firewalls, isolation)?

ii. If not, why? Are there any plans to eventually segment these systems?

b. How do you secure any remote access to the OT system?

17. What is your process for collating information on the multiple malfunctions in different areas of the facility?

Module 2: Detection & Response

Day 28, 6:00 a.m.

A water pump begins repeatedly turning itself off and on. The central computer is unable to communicate with the water pump to enact the emergency shutoff procedure. Subsequently, the water pump breaks, putting the system at risk of low pressure.

Day 28, 8:00 a.m.

All control system indicators point to a potential hazardous materials (hazmat) situation in which the chlorination of the water appears to be reaching a dangerous, unsafe level. Fail-safe protection systems for ozone generators and chlorine feeds at [Water System] facilities are activated to shut down distribution operations.

Discussion Questions

1. What steps would your organization take in response to these events?
2. How would you determine if the broken pump was caused by a mechanical malfunction, an accidental cyber issue, or an intentional act of sabotage?
    a. How would this incident be investigated?
    b. What are the internal and external communications processes?
3. What actions would [Water System] take in response to the broken water pump?
    a. What internal and external resources are needed to respond?
4. What steps must be taken to “go manual”? How long does this take and how long can manual operations be sustained?
    a. What are the water system limitations in manual mode?
    b. Can you maintain full pressure and full treatment?
5. How does the recovery time objective for replacing the broken pump impact the water system?
6. What is the decision-making process for identifying which threats are communicated to customers and which do not rise to that level?
7. What messaging, if any, is your organization providing to the public regarding these mechanical malfunctions?
    a. What information are you passing on to regulatory, law enforcement, other water utilities or information sharing groups?

Day 28, 9:30 a.m.

Some employees of [Water System] report latency and missing programs on their computers. The IT department notes that several of the employees experiencing latency and missing programs clicked on the link in the suspicious HR training email.

Day 29, 9:00 a.m.

A reporter from a local news station contacts the [Water System], saying a source told him that valves at several other water system facilities in the region have been malfunctioning. The reporter asks if your organization has been experiencing similar issues.

Day 29, 9:30 a.m.

A disgruntled employee posts inflammatory statements about the [Water System] on social media, claiming that the facility has been mismanaged for months and that water quality is not a priority. These posts are shared numerous times across social media platforms.

Day 29, 10:00 a.m.

Internet bloggers start posting similar accusations regarding the region's water supply.

Day 29, 11:00 a.m.

State agencies and local city websites are defaced with the message, "Your water is wasted!" before the messages are taken offline. City officials, county commissioners, and school district officials receive Facebook invites to the "Water is Wasted Party" from a user named "Rainmaker."

Discussion Questions

8. How would you address the issues of latency and missing programs?

9. What would your organization tell the reporter about the malfunctioning valves?

10. How would your organization respond to the social media posts by the disgruntled employee?

11. Does your organization have a Communications Plan?

    a. Are your public relations personnel trained in cybersecurity terminology?

    b. Do they have pre-scripted messages to respond to a cyber-related event?

12. At this point, what is your public messaging strategy?

    a. Who coordinates and approves your messaging?

    b. What actions, if any, would your organization take in response to the public accusations regarding the water supply?

13. What legal liabilities do you face as an organization?

14. What capabilities and resources are required for responding to this series of incidents?

    a. What internal resources do you depend on? Are your current resources sufficient?

    b. Whom do you contact if you need additional third-party assistance?

    c. What resources are available within the state or locally? How do you request these resources?

    d. What federal resources are available? How are these requested?

Day 30, 8:00 a.m.

[Water System]'s network administrator notices an above average amount of outbound network traffic coming from several ports. Upon investigation, they discover that a large amount of data was transferred in the outbound network traffic.

Day 30, 9:00 a.m.

Employees at [Water System] report to IT that their computers are freezing, and work devices begin shutting down. When attempting to restart devices, employees are locked out of their machines and their screens display a ransomware message that reads:

> "Oops! Your files have been encrypted by RAINMAKER. Pay what you think they're worth and your files might be returned. Please submit payment to the wallet below within 72 hours or everything will be deleted."

Day 31, 8:00 a.m.

A hacker group called "Rainmaker" is now publicly claiming responsibility for the attack, taking to social media and describing the attack against [Water System]. They claim to have stolen customer billing data and post a link with a sample of the stolen data to a site on the dark web known to be used by cybercriminals.

Discussion Questions

18. How would you address the above average amount of outbound network traffic and apparent data transfer?
19. What actions would you take following the potential disclosure of customer data?
20. Does your organization have a documented policy for ransomware?
21. Do you pay the ransom? Why or why not?
    a. Who decides? If yes, how do you pay? How much do you pay?
    b. What are the advantages/disadvantages?
    c. What are the legal and reputational ramifications?
22. If you have a cybersecurity insurance policy, what are its requirements for ransomware?
    a. Are the requirements integrated into your incident response plans?

Module 3: Recovery

Day 31, 9:00 a.m.

[Water System] is inundated with calls from customers, concerned that their billing information has been compromised. Others are worried that they will be unable to make payments and their water service will be discontinued.

Day 31, 10:00 a.m.

The Assistant Director and Chief Operator of [Water System] have both received emails and phone calls from the [State Primary] Agency and the Environmental Protection Agency (EPA) requesting information on the recent attacks on [Water System] and when they should expect [Water System] to resolve the issue and return to its normal state of operations.

Discussion Questions

1. How would you respond to your customers’ concerns about their billing information?
2. How would you respond to the requests for information from the [State Primary] Agency and the EPA?
3. What backup systems are utilized by your organization?
    a. How quickly can they be deployed?
    b. How often are backups created or updated?
    c. How often do you test restoring from backups?
4. What systems would be prioritized for recovery efforts? How was this decision made?
5. Are your internal resources adequate to handle this scenario, or will you need to bring in external assistance?
    a. How would you request them?
6. Have you established a quantifiable, repeatable process for determining when an incident is resolved and when the incident response team can stand down?
7. Describe your After-Action Report or lessons learned process.
    a. How are recommended improvements implemented and tested?

Appendix A: Additional Discussion Questions

The following section includes supplemental discussion questions to guide exercise play. Questions are aligned to the NIST functional areas and leadership roles. Exercise planners are encouraged to select additional, applicable discussion questions to the chosen scenario to bolster participant conversation. *This instructional page, as well as undesired discussion questions, should be deleted.*

Identify

1. Has your organization conducted a cyber risk assessment to identify organization-specific threats and vulnerabilities?
    a. What are your most significant threats and vulnerabilities?
    b. What are your highest cyber security risks?
2. How does your organization integrate cybersecurity into the system development life cycle (i.e., design, procurement, installation, operation, and disposal)?
3. Discuss the role of cybersecurity in contracts with third-party support vendors and crucial suppliers. Have you discussed these types of concerns and risks with them?
4. Discuss your supply chain concerns related to cybersecurity.
5. What role does organizational leadership play in cybersecurity? Does this role differ during steady-state and incident response?
6. What level of funding and/or resources are devoted to cyber preparedness? Based on your risk assessment, what is the range of potential losses from a cyber incident?
7. Discuss cyber preparedness integration with your current all-hazards preparedness efforts. Who are your cyber preparedness stakeholders (public, private, non-profit, other)?
8. What mission essential functions depend on information technology and what are the cascading effects of their disruption?
9. Have you had any external review or audit of your IT plans, policies, or procedures within the last year?
10. Discuss the current network security architecture for crucial suppliers with remote access.
11. Are background checks conducted for IT, security and key supporting personnel?
12. Is there a manager/department in charge of cybersecurity management? If yes, is this the primary function of that manager?
13. How does your organization recruit, develop, and retain cybersecurity staff?
14. Would your organization receive the information presented in the scenario?
    a. Through what channels would this information be received and disseminated?
    b. Are there established mechanisms to facilitate rapid information dissemination?
    c. Are there known communication gaps? If so, who in your organization is responsible for addressing those gaps?
    d. What actions, if any, would your organization take based on this information?
15. What other sources of cybersecurity threat intelligence does your organization receive? For example, information from Federal Bureau of Investigation (FBI), InfraGard, open source reporting, security service providers, others?
    a. What cyber threat information is most useful?
    b. Is the information you receive timely and actionable?
    c. Who is responsible for collating information across the organization?

16. What mechanisms and products are used to share cyber threat information within your organization and external to your organization (e.g., distribution lists, information sharing portals)?
17. Describe how variables in threat information (timeframe, credibility, and specificity) impact decision making.
18. How well-defined is cybersecurity in relation to contracts with third-party support vendors and crucial suppliers?
    a. How often are contracts reviewed?
    b. How well do your service level agreements address incident response?

Protect

1. Does your organization have established cybersecurity governance? When was it signed?
2. How is cybersecurity integrated into both organizational and project risk assessments and management?
3. Does your organization employ a formal sanctions process for personnel failing to comply with established information security policies and procedures? If so, has this been communicated to employees?
4. Does your organization have a cybersecurity incident response plan? When was it issued? When was the incident response plan last revised? What authorities require which departments or agencies to follow the plan?
5. Does your organization utilize multi-factor authentication to mitigate the potential effects of phishing?
6. Does your IT department have a patch management plan in place? If so:
    a. Are risk assessments performed on all servers on the network?
    b. Are processes in place to proactively evaluate each server's criticality and applicability to software patches?
    c. Does this plan include a risk management strategy that addresses the following considerations?
        i. The risks of not patching reported vulnerabilities?
        ii. Extended downtime?
        iii. Impaired functionality?
        iv. The loss of data?
7. What active measure(s) does your organization employ to prevent denial of service (DDoS) attacks against your websites and operational systems?
8. Do you have a method for tracking and/or identifying problematic pieces of firmware in your organization, should a vulnerability be identified?
9. What processes does your organization have in place for when an employee is terminated or resigns?
    a. Are there any additional processes that are implemented if the employee's termination is contentious?
    b. Does your organization retrieve all information system-related property (e.g., authentication key, system administration's handbook/manual, keys, identification cards, etc.) during the employment termination process?

10. Do any third-party vendors have unmitigated access into your network?
    a. What protections do you have in place to protect against malicious intent by those vendors or outside parties that have access to your network?
11. Discuss the status of cyber preparedness planning within your organization.
    a. Have you completed a business impact analysis? Does the analysis include IT infrastructure supporting mission essential functions identified in continuity of operations and continuity of government plans?
    b. Is cybersecurity integrated in your business continuity plans? Does your business continuity and/or disaster recovery planning have a prioritized list of information technology infrastructure for restoration?
    c. How have IT specific plans been coordinated with other planning efforts such as an Emergency Operations Plan or Continuity of Operations Plan?
12. What are your identified responsibilities for, and capabilities to, prevent cyber incidents?
13. Who is responsible for network and information security management?
14. Does your Emergency Operations Plan have a Cyber Incident Annex? When was it last revised? Who is responsible for maintaining the annex?
15. Can you identify key documents that support cyber preparedness at a federal, state, or local level? (Presidential Policy Directive (PPD) 41: United States Cyber Incident Coordination, National Cyber Incident Response Plan (NCIRP), PPD 21: Critical Infrastructure Security and Resilience, Executive Order: Improving Critical Infrastructure Cybersecurity, National Response Framework (NRF), National Infrastructure Protection Plan (NIPP), National Institute of Standards and Technology (NIST) Cybersecurity Framework, etc.)
16. Does your organization follow a cybersecurity standard of practice (NIST Cybersecurity Framework/800 Series, ISO/IEC, etc.)? If so, which?
17. Are there flowcharts showing the high-level relationships and crisis lines of communication (i.e., who calls who) specifically for a cyber incident? Are they part of the response or continuity planning documents?
18. Does your organization have a formal or informal policy or procedures pertaining to IT account management?
    a. Do these policies or procedures include protocols for establishing, activating, modifying, disabling, and removing accounts?
    b. Do these policies or procedures include protocols/steps for notifying IT account managers/administrators when users are terminated?
19. Are IT and business continuity functions coordinated with physical security? Are all three then collaborating with public relations, human resources, and legal departments?
20. Do you have processes to ensure that your external dependencies (contractors, power, water, etc.) are integrated into your security and continuity planning and programs?
21. Describe the decision-making process for protective actions in a cyber incident. What options are available? Have these options been documented in plans? How are they activated?
22. What immediate protection and mitigation actions would be taken at your organization in this scenario? Who is responsible for those actions?
23. What protective actions would you take across non-impacted systems or agencies in the scenario presented? Who is responsible for protective action decision-making? How are actions coordinated across parts of the organization?

24. Compare and contrast physical and cyber incident notifications and protective action decision-making.

Detect

1. How do employees report suspected phishing attempts?
    a. What actions does your department take when suspicious emails are reported?
    b. Are there formal policies or plans that would be followed?
    c. Does your department conduct phishing self-assessments?
2. What process does the general workforce follow to report suspected cyber incidents? Is this a formal process on which they have been trained?
3. Do you have defined cybersecurity incident escalation criteria, notifications, activations, and/or courses of action?
    a. If so, what actions would be taken at this point? By who?
    b. Would leadership be notified?
4. How does your organization baseline network activity? How would you be able to distinguish between normal and abnormal traffic?
5. Does the organization report cybersecurity incidents to outside organizations? If so, to whom? What, if any, mandatory reporting requirements do you have?
6. At what point would your organization begin to suspect the HVAC/fire alarm issues might be the result of malicious cybersecurity activity?
7. If you were one of the individuals who received the email demanding bitcoin payment, who would you inform, internally? Who, if anyone would you inform externally?
8. Do detection and analysis procedures differ for loss of personally identifiable information (PII), phishing attempts, data exfiltration, data modification, or other incidents?
9. Would this be considered the most severe tier of security incident for your organization? What, if any, additional notifications or actions would this prompt?
10. Who is responsible for correlating information across different organizational-level incidents?
11. What resources and capabilities are available to analyze the intrusions:
    a. Internally?
    b. Externally though government partners?
    c. Through the private sector?
12. How is information shared among your internal and external stakeholders? Through formal or informal relationships? What information sharing mechanisms are in place?
13. Discuss your organization’s intrusion detection capabilities and analytics that alert you to a cyber incident.
14. What type of hardware and/or software does your organization use to detect/prevent malicious activity of unknown origin on your systems/network?

Respond

1. What is your planned cyber incident management structure?
    a. Who (by department and position) leads incident management and why?
    b. How are they notified?
    c. When did they last exercise their role?
    d. What is the length of your operational period (i.e., your “battle rhythm”)?

e. What are the primary and contingency communication mechanisms necessary to support incident management?

2. Do you have someone within your organization who monitors the Dark Web? If so, how would you verify the security researcher’s claims and confirm authenticity of the sensitive information in question?
3. What level of leadership/management would be notified at this point in the scenario? Is there a plan in place detailing the thresholds at which different notifications are made and what information is provided?
4. What is your department or agency’s primary concern? Mitigation of the incident (resolving the issue) or investigation (preserving the evidence to build a criminal case)? Who would make this decision? Are these mutually exclusive?
5. What response actions would your organization have taken at this point? Are these actions driven by a plan?
6. What impact will the sale of sensitive or PII have on your response and recovery activities?
   a. Will IT alert authorities? Have your public relations priorities changed?
   b. Will it trigger any additional legal or regulatory notifications?
7. Whom will you notify, internally and externally, of these incidents?
   a. Is there a process or plan in place that outlines the severity thresholds for which different notifications are made and what information is to be conveyed?
   b. Are you keeping senior leadership updated? What information is provided and how is it communicated?
   c. Would you make any notification to the public?
      i. If so, how are you coordinating your messaging within your organization?
      ii. Do you have pre-canned messaging or holding statements for such an event?
8. How are you ensuring unity of message between your organization, the public sector, and elected officials?
9. How would these events affect your organization’s business operation/processes?
10. Would any of these issues be considered a cyber incident at this point?
11. Do these incidents generate any concerns that have not been addressed?
12. How would your organization respond to the discovery of a malicious, unauthorized administrator account on your systems? Who would be informed internally? Who would be informed externally (e.g. law enforcement, cybersecurity insurance partners, etc.)?
13. What resources are required for incident investigation and attribution? Are sufficient resources available in-house?
14. Would the events presented in the scenario trigger activation of your emergency operations plan cyber incident annex? If so, would that alter any roles and responsibilities?
   a. At what point in the scenario would you contact law enforcement and/or the state Attorney General?
   b. How would relationships with law enforcement and other partners be managed? Where is the process documented?
   c. How does a law enforcement investigation impact containment, eradication, and recovery efforts?
15. Are processes and resources in place for evidence preservation and collection?
16. Discuss the difference between network and host forensics. How are you equipped and staffed to address this?

17. Do you have a network operations center? Security operations center? What are their roles during a response?
18. What are your essential elements of information and key information questions necessary for operational and executive-level responses to cyber incidents?
19. What mission essential functions are impacted by the incidents described in the scenario?
20. Is there a way to maintain service availability of key assets (e.g., network connectivity, etc.)?
    a. What capabilities and resources are required for responding to this series of incidents?
    b. What internal resources do you depend on? Are your current resources sufficient?
    c. Whom do you contact if you're in need of additional third-party assistance?
    d. What resources are available within the state or locally? How do you request these resources?
    e. Do you have personnel tasked with incident response or a designated cyber incident response team within your organization?
        i. If so, what threshold must be reached for the cyber incident response personnel to be activated? Does this scenario reach that threshold?
        ii. Who is responsible for activating the cyber incident response personnel and under what circumstances?
        iii. What are the cyber incident response team/personnel's roles and responsibilities?
21. Does this exceed your organization's ability to respond?
    a. If so, are there established procedures to request additional support?
22. What are your organization's response priorities?
    a. Who would be notified at this point in the scenario? Is there a plan in place detailing the thresholds at which different notifications are made and what information is provided?
    b. What response actions would the IT/IS department take at this point? Are these actions driven by a plan?
    c. What response capabilities and resources are required to respond to these incidents?
23. What actions would be taken when the exfiltration is discovered? Does your organization have written plans that would be implemented?
24. Do you pay the ransom?
    a. Who decides?
    b. What's the process?
    c. What are the advantages/disadvantages to paying?
    d. What are the political ramifications?
    e. What outside partners/entities do you need to contact?
25. Where do you receive cyber response technical assistance? Do you have plans, procedures or policies in place to access this assistance?
26. Have you proactively identified and established the service provider relationships needed for incident/breach response issues (e.g., credit counseling, forensic/computer security services)?
    a. What are some challenges that are experienced by information technology and business continuity planning in terms of information sharing?
    b. Is information flowing in both directions?
27. What processes are used to contact critical personnel at any time, day or night?
    a. How do you proceed if critical personnel are unreachable or unavailable?

Recover

1. When does your organization determine a cyber incident is closed?
    a. Who makes this decision?
    b. Would your organization engage in any post-incident activities?
2. What actions would your organization take if your IT/incident response staff could not confirm the integrity of your systems/data?
    a. Would senior leaders consider re-activating critical business processes and systems? What is the risk associated with doing so?
    b. Would your organization consider a complete rebuild of these systems? How long and costly would that process be?
    c. What factors do you consider when making these decisions?
3. What formal policies and procedures does your organization use to decide when and how to restore backed-up data, including measures for ensuring the integrity of backed-up data before restoration?
4. Does your organization have back-ups of vital records in a location that is separated from your primary working copies of your files?
    a. How long do you keep any copies of archived files backed up?
    b. How long of a downtime would exist between your primary files and the restoration of files via your back-up?
5. Are redundant systems in place if the impacted system(s) is compromised?
6. Describe your role in post-incident activity.
7. How would you work with critical infrastructure providers to determine the incident is over?
8. How does post incident-activity differ when critical infrastructure is involved?
9. Does your organization have a continuity of operations plan (COOP) for conducting its functions at a location other than your main building?
    a. If so, how would a suspected cyber incursion impact your organization's ability to activate its COOP Plan?
10. Are alternative systems or manual processes in place to continue operations if a critical system is unavailable for a significant period of time?
    a. Who can authorize use of alternate systems or procedures?

Training and Exercises

1. Does your organization provide basic cybersecurity and/or IT security awareness training to all users (including managers and senior executives)?
    a. How often is training provided? Does it cover:
        i. Review of department and/or agency acceptable use and IT policies,
        ii. Prominent cyber threat awareness,
        iii. Password procedures, and
        iv. Whom to contact and how to report suspicious activities?
    b. Is training required to obtain network access?
    c. What security-related training does your department or agency provide to, or contractually require of, IT personnel and vendors with access to your city's or county's information systems? How often do they receive the training?
2. Do your cybersecurity incident response team members undergo any special training to detect, analyze, and report this activity? If so, can you describe this training?

    a. Is your staff sufficiently trained to read and analyze your intrusion detection system logs?

3. What training do you provide in support of your Cybersecurity Incident Response Plan, Business Continuity Plan, Emergency Operations Plan Cyber Incident Annex, or other related plans?
    a. Do employees know what constitutes suspicious cybersecurity activities or incidents?
    b. Do they know what actions to take when one arises?
4. If you have a cyber incident response plan, how often does your organization exercise the plan?
    a. Who is responsible for the exercise planning?
    b. What agencies are involved in the exercise?
    c. What level of the organization is required to participate?
    d. What actions follow the exercise?
5. How do your organization's annual Training and Exercise Planning Workshop and Multi-Year Training and Exercise Plan address cybersecurity?
6. What are your cybersecurity incident response team's exercise requirements?
7. Do your organization's exercise efforts include both physical and cyber risks?
8. Have senior or elected officials participated in a cybersecurity exercise?
9. Are there additional training and/or exercising requirements for your organization?

Senior Leaders and Elected Officials

1. What is your cybersecurity culture? As a leader in your organization, what cybersecurity goals have you set? How have they been communicated?
2. As it relates to your jurisdiction, what cybersecurity information do you request? What do you receive?
3. What are your cybersecurity risks?
4. Who develops your jurisdiction's cybersecurity risk profile? What are their reporting requirements? Are they directed to, required by statute, or other? How often do they report?
5. Is your cybersecurity risk integrated with physical risk for an integrated jurisdictional risk assessment?
6. What is your jurisdiction's greatest cybersecurity concern? Why do you rate this concern as your greatest concern? Who reports to you on cyber threats?
7. What, if any, infrastructure does your jurisdiction own, operate, and/or regulate?
8. What relationships do you have with critical infrastructure owners and operators?
9. What priorities have you set related to the cybersecurity of critical infrastructure?
10. What is your most important critical infrastructure?
11. What are your regulatory requirements related to critical infrastructure, if any?
12. What is the greatest threat facing your critical infrastructure? What, if anything, is your jurisdiction able to do to mitigate it?
13. When did you last receive a cyber threat briefing for your jurisdiction?
14. How has your jurisdiction prepared for a cyber incident?
    a. Does your jurisdiction have cybersecurity plans in place? How many information security officers do you have?
    b. Does the plan indicate how they will work together?
15. Have your information security officers and emergency managers jointly planned for cybersecurity incidents?
16. What are your cybersecurity workforce gaps? How does your jurisdiction recruit, develop, and retain cybersecurity staff?

17. What cybersecurity training do you have planned for cybersecurity staff, managers, and general workforce?
18. What magnitude of incident would require your notification? How does that notification process work? Is it planned?
19. What requirements or agreements, if any, exist for critical infrastructure to notify you of a cyber incident?
20. Who advises you on cyber threats? What are your essential elements of information or critical information requirements?
21. What is your planned role in protective action decision-making?
22. What is your planned cyber incident management structure? What parts of the government need to be engaged?
23. Would your jurisdiction's Emergency Operations Center be activated in a cyber incident? How? Why?
24. What is your role in a cyber incident?
25. How does a law enforcement investigation impact your response?
26. What is your role in communicating to the public?
27. How are costs of the response calculated?
28. What information do you need to support your decision-making process?
29. Who is your jurisdiction's cybersecurity liaison to privately-owned and operated critical infrastructure?
30. What are your expectations of the State and Federal Government?
31. Describe your role in post-incident activity.
32. What is your role in restoring and/or maintaining public confidence?

Media

1. What are your public affairs concerns? Who is responsible for coordinating the public message? Is this process a part of any established plan?
    a. How would your department respond to the local media reports?
    b. What information are you sharing with citizens? Employees?
    c. Are public information personnel trained to manage messaging related to cyber incidents?
    d. Does your department have pre-drafted statements in place to respond to media outlets?
    e. Are they trained to manage your social media presence?
    f. Are all personnel trained to report any contact with the media to appropriate public information personnel?
2. What information would your organization communicate to the public?
3. Who is responsible for public information related to the incident? What training or preparation have they received?

Legal

1. What are the legal issues you must address?
2. What policies should your organization have? Does it exercise these policies? If so, how often?
3. What legal documents should your organization have in place (for example with third-party vendors)?
4. What is the role of the legal department in this scenario?
5. Does your state have security breach notification laws? If so, what do they include?

Appendix B: Acronyms

Acronym	Definition
CISA	Cybersecurity and Infrastructure Security Agency
COOP	Continuity of Operations Plan
DHS	U.S. Department of Homeland Security
EPA	Environmental Protection Agency
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
HR	Human Resources
HVAC	Heating, Ventilation, and Air Conditioning
IEC	International Electrotechnical Commission
IP	Internet Protocol
IS	Information Systems
ISO	International Organization for Standardization
IT	Information Technology
NCIRP	National Cyber Incident Response Plan
NIPP	National Infrastructure Protection Plan
NIST	National Institute of Standards and Technology
NRF	National Response Framework
OT	Operational Technology
PII	Personally Identifiable Information
POC	Point of Contact
PPD	Presidential Policy Directive
TV	Television
TLP	Traffic Light Protocol
VLAN	Virtual Local Area Network
WaterISAC	Water Information Sharing and Analysis Center

Appendix C: Case Studies

Remote Access Attack Attempts to Poison City Water Supply

In February 2021, an attacker gained access to a Florida city's water treatment system and attempted to increase the amount of sodium hydroxide present in the water to 111 times the normal level. The attacker gained remote access to the system through TeamViewer due to poor password security practices. An operator at the plant noticed the change and was able to restore the sodium hydroxide levels back to a safe level before any harm was done. The public was not at risk from this attack, since the changes needed 24-36 hours to take effect, and redundancies had been designed to notify operators about unsafe sodium hydroxide levels. Private investigation by a cybersecurity firm revealed that the website of a Florida water infrastructure construction company was set up as a watering hole and accessed by a water treatment employee hours before the attack. However, there is no evidence that the watering hole played any part in the TeamViewer compromise. The city has since taken further precautions to prevent more unauthorized access to the water treatment system. A county Sheriff's Office and the FBI are jointly investigating the incident.[2,3]

Remote Access Attack Attempts to Stop Water Treatment

In January 2021, a hacker gained access to the computer system at a California water treatment plant through TeamViewer, using the credentials of a former employee. Once the attacker gained access, they deleted programs the plant used to treat drinking water. The attack was not noticed by employees until the next day. In response, the plant changed all passwords and reinstalled the deleted programs. Several news outlets reported that the attacker attempted to poison the water supply, but a spokesperson from Northern California Regional Intelligence Center denies this claim. The attack did not cause any failures in the water supply and the water remained safe to drink.[4,5]

Ransomware Attack Leaves Customers Unable to Pay Their Water Bills

In May 2019, a ransomware attack disabled the majority of a Maryland city's servers, including those used to create and send water bills to around 200,000 customers. The ransom note identified the ransomware as RobbinHood and requested 13 Bitcoin, worth over $75,000 at the time. The relatively small demand suggests that this attack was not specifically targeted at the city. The city was unable to send water bills to customers for three months after the ransomware attack. Since these bills accounted for three months of service, they were very high and posed financial burden to some families. During the three months of no payments, the city water supply remained operational due to money reserves. The city was assisted by the FBI following the attack.[6,7]

Water Reclamation District Hit with Ransomware Attack

In March 2016, a Nevada county's water reclamation district experienced a ransomware attack. In response, the facility contacted their IT department and shut down their computers. The water

[2] (Kovacs, 2021)

[3] (Vera, Lynch, & Carrega, 2021)

[4] (Collier, 2021)

[5] (Crump, 2021)

[6] (Duncan, Baltimore's water department waits for revenue as customers wait for large bills after ransomware freezes system, 2019)

[7] (Duncan & Campbell, Baltimore city government computer network hit by ransomware attack, 2019)

treatment plants remained functional and no customer or employee information was compromised. Law enforcement was notified of the incident and the FBI was asked to investigate. The ransom amount was not disclosed, and it is unclear whether the city paid it. The full resolution to the incident has not been made known.[8,9]

[8] (Associated Press, 2016)

[9] (Barnes, 2016)

Appendix D: Attacks and Facts

Social Engineering

One of the most prominent tactics attackers use to exploit network and system vulnerabilities is social engineering–the manipulation of users through human interaction and the formation of trust and confidence to compromise proprietary information. Techniques for uncovering this information largely involve the use of phishing, i.e. email or malicious websites that solicit personal information by posing as a trustworthy source. Social engineering is effective for breaching networks and evading intrusion detection systems without leaving a log trail and is completely dependent on the operating system platform. While technical exploits aim to bypass security software, social engineering exploits are more difficult to guard against due to the human factor. Organizations should take steps towards strengthening employee cybersecurity awareness training, to include training personnel to be cautious of suspicious emails, know where to forward them and keeping software and systems up-to-date.

Additional Resources

- Avoiding Social Engineering and Phishing Attacks (https://www.us-cert.gov/ncas/tips/ST04-014)
- The Most Common Social Engineering Attacks (https://resources.infosecinstitute.com/common-social-engineering-attacks/)

Ransomware

Ransomware is a type of malware that denies access to victims' data or systems through encryption with a key only known by the malicious actor who deployed the malware. Once encrypted, the ransomware directs the victim to pay the attacker, typically in the form of cryptocurrency, so the victim can receive a decryption key. Ransomware typically spreads through phishing emails or by unknowingly visiting an infected website. Recovery can be an arduous process and there is no guarantee the victim will receive access to their data or systems if the ransom is paid. For more information on best practices to protect users from the threat of ransomware, as well as recent Alerts on specific ransomware threats, see the resource list below.

Additional Resources

- CISA Ransomware (Stop Ransomware | CISA)
- Protecting Against Ransomware (https://www.us-cert.gov/ncas/tips/ST19-001)
- Indicators Associated With WannaCry Ransomware (https://www.us-cert.gov/ncas/alerts/TA17-132A)
- Incident trends report (Ransomware) (https://www.ncsc.gov.uk/report/incident-trends-report#ransomware)

Appendix E: Doctrine and Resources

Laws

- National Cybersecurity Protection Act of 2014 (Dec 2014) https://www.congress.gov/113/plaws/publ282/PLAW-113publ282.pdf
- Federal Information Security Modernization Act of 2014 (Dec 2014) https://www.dhs.gov/fisma
- OMB Memorandum: M-15-01, Fiscal Year 2014-2015: Guidance on Improving Federal Information Security and Privacy Management Practices (Oct 2014) https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2015/m-15-01.pdf

Presidential Directives

- Executive Order 13800: Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure (May 2017) https://trumpwhitehouse.archives.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/
- Presidential Policy Directive-41: United States Cyber Incident Coordination (Jul 2016) https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident
- Annex to Presidential Policy Directive 41: Annex to the Directive on United States Cyber Incident Coordination (Jul 2016) https://www.hsdl.org/?view&did=797545
- Presidential Policy Directive 8: National Preparedness (Mar 2011), (Updated Sep 2015) https://www.dhs.gov/presidential-policy-directive-8-national-preparedness
- Presidential Policy Directive 21: Critical Infrastructure Security and Resilience (Feb 2013) https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil
- Executive Order 13636: Improving Critical Infrastructure Cybersecurity (Feb 2013) https://www.hsdl.org/?view&did=731040

Strategies and Frameworks

- National Cyber Incident Response Plan (Dec 2016) https://www.us-cert.gov/ncirp
- National Cyber Strategy of the United States of America (Sep 2018) https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf
- U.S Department of Homeland Security Cybersecurity Strategy (May 2018) https://www.hsdl.org/?view&did=810462
- Framework for Improving Critical Infrastructure Cybersecurity (Apr 2018) https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
- National Protection Framework, Second Edition (Jun 2016) https://www.fema.gov/sites/default/files/2020-04/National_Protection_Framework2nd-june2016.pdf
- Office of Management and Budget (OMB) Memorandum: M-16-04, Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government (Oct 2015)

https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2016/m-16-04.pdf

Key Points of Contact

- Department of Homeland Security/Cybersecurity and Infrastructure Security Agency (CISA) (contact: central@cisa.dhs.gov)
- Federal Bureau of Investigation (FBI)
    - Field Office Cyber Task Forces (contact: https://www.fbi.gov/contact-us/field-offices)
    - Internet Crime Complain Center (IC3) (contact: http://www.ic3.gov)
    - National Cyber Investigative Joint Task Force (NCIJTF) CyWatch 24/7 Command Center (contact: cywatch@ic.fbi.gov; (855) 292-3937)
- United States Secret Service Field Offices and Electronic Crimes Task Force (ECTFs) (contact: https://www.secretservice.gov/contact/field-offices/)

Other Available Resources

- Multi-State Information Sharing and Analysis Center (MS-ISAC) (contact: info@msisac.org; (518) 266-3460)
- Cybersecurity and the States (National Association of State Chief Information Officers [NASCIO]) (http://www.nascio.org/Advocacy/Cybersecurity)
- National Governors Association (NGA) (https://www.nga.org/)
- DHS Cybersecurity Fusion Centers (https://www.dhs.gov/state-and-major-urban-area-fusion-centers)
- InfraGard (https://www.infragard.org/)
- Internet Security Alliance (http://www.isalliance.org/)
- Information Sharing and Analysis Centers (ISACs) and Information Sharing and Analysis Organizations (ISAOs) (https://www.isao.org/information-sharing-groups/)
    - International Association of Certified ISAOs (http://www.certifiedisao.org; contact: operations@certifiedisao.org)
    - National Council of ISACs (https://www.nationalisacs.org/)

References Cited

Associated Press. (2016, March 8). *Cyber Attack Hits Clark County Water Reclamation District*. Retrieved June 25, 2021, from Nevada Public Radio: https://knpr.org/headline/2016-03/cyber-attack-hits-clark-county-water-reclamation-district

Barnes, B. (2016, March 8). *Clark County Water Reclamation District Computer System Hacked*. Retrieved June 25, 2021, from Las Vegas Review Journal: https://www.reviewjournal.com/local/local-las-vegas/clark-county-water-reclamation-district-computer-system-hacked/

Collier, K. (2021, June 17). *A Hacker Tried to Poison a Calif. Water Supply. It Was as Easy as Entering a Password.* Retrieved June 25, 2021, from NBC News: https://www.nbcnews.com/tech/security/hacker-tried-poison-calif-water-supply-was-easy-entering-password-rcna1206

Crump, J. (2021, June 18). *Hackers Tried to Poison California Water Supply in Major Cyber Attack*. Retrieved June 25, 2021, from Newsweek: https://www.newsweek.com/san-francisco-water-plant-hack-cyber-attack-poison-supply-1601798

Duncan, I. (2019, July 12). *Baltimore's water department waits for revenue as customers wait for large bills after ransomware freezes system*. Retrieved June 25, 2021, from The Baltimore Sun: https://www.baltimoresun.com/politics/bs-md-ci-water-bills-ransomware-20190712-2qzqu4yg5vguxefriiiagahece-story.html

Duncan, I., & Campbell, C. (2019, May 7). *Baltimore city government computer network hit by ransomware attack*. Retrieved June 25, 2021, from The Baltimore Sun: https://www.baltimoresun.com/politics/bs-md-ci-it-outage-20190507-story.html

Kovacs, E. (2021, May 19). *Probe Into Florida Water Plant Hack Led to Discovery of Watering Hole Attack*. Retrieved June 25, 2021, from SecurityWeek.com: https://www.securityweek.com/probe-florida-water-plant-hack-led-discovery-watering-hole-attack

Palo Alto Networks. (2021). *What Is Network Segmentation?* Retrieved June 28, 2021, from Palo Alto Networks: https://www.paloaltonetworks.com/cyberpedia/what-is-network-segmentation

Vera, A., Lynch, J., & Carrega, C. (2021, February 8). *Someone tried to poison a Florida city by hacking into the water treatment system, sheriff says*. Retrieved June 25, 2021, from CNN: https://www.cnn.com/2021/02/08/us/oldsmar-florida-hack-water-poison/index.html