

**CISA Tabletop Exercise Package– Water/Wastewater Systems**

[Enter Organization Name]

<Exercise Date>

Updated November 2023

Cybersecurity and Infrastructure Security Agency

Table of Contents

[Handling Instructions 3](#_Toc150425180)

[Exercise Overview 5](#_Toc150425186)

[General Information 6](#_Toc150425187)

[Module 1 8](#_Toc150425188)

[Module 2 10](#_Toc150425189)

[Appendix A: Additional Discussion Questions 12](#_Toc150425190)

[Appendix B: Acronyms 16](#_Toc150425191)

[Appendix C: Case Studies 17](#_Toc150425192)

[Appendix D: Attacks 18](#_Toc150425193)

[Appendix E: Contacts and Resources 19](#_Toc150425194)

# Handling Instructions

**Delete instructions that are not applicable.**

TLP:CLEAR

The title of this document is <Exercise Title> Situation Manual. This document is unclassified <if applicable> and designated as “*Traffic Light Protocol (TLP):CLEAR*”: Recipients can spread this to the world; there is no limit on disclosure. This designation is used 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:CLEAR information may be shared without restriction.**

This document may be disseminated publicly pursuant to TLP:CLEAR 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>.

TLP:GREEN

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, recipients can spread this within their community. This designation is used when information is useful to increase awareness within their wider community. Recipients may share TLP:GREEN information with peers and partner organizations within their community, but not via publicly accessible channels. TLP:GREEN information may not be shared outside of the community. **Note: When “community” is not defined, assume the cybersecurity/cyber defense 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:AMBER

The title of this document is <Exercise Title> Situation Manual. This document is unclassified <if applicable> and designated as “*Traffic Light Protocol (TLP):AMBER”:* Limited disclosure, recipients can only spread this on a need-to-know basis within their organization and its clients. This designation is used when information requires support to be effectively acted upon, yet carries risk to privacy, reputation, or operations if shared outside of the organizations involved. Recipients may share TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm.

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:AMBER+STRICT

The title of this document is <Exercise Title> Situation Manual. This document is unclassified <if applicable> and designated as *“Traffic Light Protocol (TLP):AMBER+STRICT*: Limited disclosure, recipients can only spread this on a need-to-know basis within their organization. Note that “*TLP:AMBER+STRICT”* restricts sharing to the organization only. This designation is used when information requires support to be effectively acted upon, yet carries risk to privacy, reputation, or operations if shared outside of the organization involved. Recipients may share TLP:AMBER+STRICT information with members of their own organization, but only on a need-to-know basis to protect their organization and prevent further harm.

This document should be disseminated to applicable partners and stakeholders on a need-to-know basis pursuant to TLP:AMBER+STRICT 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

The title of this document is <Exercise Title> Situation Manual. This document is unclassified <if applicable> and designated as “*Traffic Light Protocol (TLP):RED*”: For the eyes and ears of individual recipients only, no further disclosure. This designation is used when information cannot be effectively acted upon without significant risk for the privacy, reputation, or operations of the organizations involved. Recipients may therefore not share TLP:RED information with anyone else. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting.

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>.

# 

# Exercise Overview

|  |  |  |
| --- | --- | --- |
| Exercise Name | Exercise Name | |
| Exercise Date, Time, and Location | Exercise Date  Time (e.g., 9:00 a.m. – 12:00 p.m.)  Exercise Location | |
| Exercise Activities | Time | Activity |
| 20 Minutes | Threat Briefing and Opening Remarks |
| 60 Minutes | Module 1 |
| 20 Minutes | Break |
| 60 Minutes | Module 2 |
| 20 Minutes | Hotwash |
| Purpose | Assess the cyber resilience of <Organization> and the ability to secure information technology (IT) and operational technology (OT) against cyber threats to the water/wastewater sector. | |
| National Institute of Standards and Technology Cybersecurity Framework Functions | Identify, Protect, Detect, Respond, Recover | |
| Objectives | 1. Assess the cyber resilience of <Organization> during and following a cyber incident impacting IT and OT. 2. Improve IT and OT cybersecurity coordination to enhance the cybersecurity posture of <Organization>. 3. Evaluate <Organization’s> ability to recover and restore operations after disruptions from cyber intrusions. | |
| Threat or Hazard | Cyber – Phishing, Insider Threat, Ransomware | |
| Scenario | During routine operations, employees receive a possibly fraudulent email, and observe potential insider threat activity and suspicious network traffic.  Customers report service disruptions, an industrial control system (ICS) failure, data is lost, and ransomware encrypts systems. | |
| Sponsor | Exercise Sponsor | |
| Participating Organizations | Overview of organizations participating in the exercise (e.g., federal, state, local, private sector, etc.). | |
| Points of Contact | |  |  | | --- | --- | | **Insert Organization POC(s)**  Contact Information | **CISA National Cyber Exercise Program (NCEP)**  [cisa.exercises@cisa.dhs.gov](mailto:cisa.exercises@cisa.dhs.gov) | | |

# General Information

## Building Resilience

The purpose of the National Cyber Exercise Program’s CISA Tabletop Exercise Packages (CTEPs) is to increase your organization’s resilience by assessing and validating capabilities and identifying areas for improvement. The National Institute of Standards and Technology (NIST) defines cyber resilience as “the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources.”[[1]](#footnote-2)

## Using this Situation Manual

Modules 1 and 2 contain the scenario injects and discussion questions you will use to conduct the exercise. There are footnotes with corresponding resources throughout the modules to guide your preparedness efforts. The appendices provide the following information to tailor the exercise discussion:

* Appendix A: Additional discussion questions that can replace or augment the existing Module 1 and 2 discussion questions.
* Appendix B: Reference section for acronyms used within this situation manual.
* Appendix C: Case studies that provide real-world examples and actionable steps taken to secure water/wastewater systems and facilities against cyber threats.
* Appendix D: An explanation of the attack types presented in this scenario.
* Appendix E: Additional cybersecurity preparedness and response resources.

## Participant Roles and Responsibilities

**Players** have an active role in discussing or performing their primary roles and responsibilities during the exercise. Players discuss or initiate actions in response to the scenario. Players may include IT/information security staff, operational technology (OT) staff, and emergency management staff.

**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. Observers may include senior-level staff such as utility management/leadership.

**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 is intended to be a multimedia, facilitated exercise. Players will participate in the following:

* Cyber threat briefing (if desired)
* Scenario modules:
  + **Module** **1:** This module introduces a possible phishing attempt, potential insider threat activity, and suspicious outbound network traffic.
  + **Module 2:** This module introduces customer services issues, ICS/SCADA failures, a ransomware attack, and data loss.
* Hotwash
* ***Structure Note:*** *Modules, timeline dates, and discussion questions included in each module may be modified as desired. Additional discussion questions for each module can be found in Appendix A.*

## Exercise Guidelines

* This exercise is intended to be held in an open, no-fault environment. Varying viewpoints are expected.
* Respond to the scenario utilizing your knowledge of existing plans and capabilities, along with the valuable 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, possible solutions, and 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.
* In any exercise, assumptions and artificialities are necessary to complete play within the given time, achieve training objectives, and account for logistical limitations. Please do not allow these factors 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

### Day 1

The Cybersecurity & Infrastructure Security Agency (CISA), Environmental Protection Agency (EPA), and the Federal Bureau of Investigation (FBI) release a joint advisory regarding a phishing campaign targeting water treatment facilities.[[2]](#footnote-3) Malicious actors have exhibited the capability to gain full system access to multiple ICS/supervisory control and data acquisition (SCADA) devices to disrupt operations and extort victims through ransom demands.

Day 4

Several employees in the information technology (IT) and operational technology (OT) departments receive an email that appears to be from your organization’s Human Resource (HR) Department.[[3]](#footnote-4) The email asks employees to log in to a website to complete a questionnaire related to employee satisfaction. Some employees report the email as suspicious, while others follow the link for the questionnaire.[[4]](#footnote-5)

### Day 10

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

### Day 17

Employees call IT complaining that their computers are running slowly, and some company applications, websites, and SharePoint are taking a while to open. Multiple login attempts are required to gain access to the network. Other employees mention that it takes several minutes to load internal SharePoint pages.

Members of your OT department conduct system maintenance in your facility. During their checks, they discover legacy OT devices that were previously marked as decommissioned but still in use. These devices should have been removed due to numerous known exploited vulnerabilities (KEV).

### Day 19

While investigating the network latency and access issues, your IT team discovers that a large amount of data was transferred in outbound network traffic to external Internet Protocol (IP) addresses. Your IT team blocks any further communication with the unknown IP addresses.

By the end of the day, your IT team discerns that a significant amount of sensitive data was exfiltrated from company file servers. The data includes employee records, customer information, and budget files that were sent to multiple external IP addresses through printer ports.[[5]](#footnote-6)

## Discussion Questions

Discussion questions included in each module are designed to explore different aspects of your operational resilience. The questions may be modified as desired. Additional questions can be found in Appendix A.

1. What cybersecurity threat information does your organization receive?
   1. What cyber threat information is most useful?
   2. How is information disseminated to relevant parties within your organization?
   3. What actions would your organization take in response to an alert like the one presented in the scenario?
2. Describe your organization’s cybersecurity training program for IT and OT employees.
   1. How often are employees required to complete this training?
   2. Describe the cross-training or the coordination between the IT and OT departments.
   3. What additional training is required for employees who have system administrator-level privileges?
   4. What type of training methods or approaches have you found most beneficial?
3. Describe your organization’s asset management plan and how you prioritize critical assets.
4. How does your organization maintain availability of key assets (e.g., network connectivity, etc.)?
5. Describe the risks/advantages to maintaining legacy equipment/systems.
   1. How do you manage technology that is no longer supported by the manufacturer?
   2. What supply chain concerns do you have regarding legacy equipment/systems?
   3. Describe your organization’s equipment commissioning and decommissioning process.
6. How do you protect IT and OT networks?
   1. What are your access control measures for both OT and IT assets and associated facilities?
   2. Do you deploy multi-factor authentication (MFA) as widely as possible for both OT and IT networks?
   3. Describe your organization’s password management policy for standard user accounts and privileged user accounts.
   4. What are the protocols for establishing, activating, modifying, disabling, and removing accounts?
7. How do employees report suspected phishing attempts or other possible cybersecurity incidents?
   1. What actions does the IT department take when suspicious emails are reported?
   2. What feedback do employees receive after reporting a suspicious email or event?

# Module 2

### Day 46

Customers call Customer Service to perform routine operations (start/stop service, pay their bill, request field visits, inquire about bill charges, etc.), but the representatives cannot access any customer information.

### Day 48

Water at your organization’s facility begins to have a chemical smell. Technicians monitoring SCADA devices report that all systems show normal readings, but a manual test of the water shows a dangerously high level of chlorine.

Later that day, technicians monitoring your organization’s various IT/OT systems notice lag and distorted data inputs that impact their ability to monitor the equipment and processes.

### Day 50

A system alarm alerts facility operators of several control valves opening and closing at random times throughout <region/state/service area>, causing a shutdown of operations due to automatic emergency fail safes.[[6]](#footnote-7) Technicians attempting to access the malfunctioning ICS/SCADA devices notice administrative account credentials were changed without their knowledge, inhibiting their access to the devices. During physical inspection of the failed components, technicians discover there is no physical reason for the failure.

### Day 51

Control panels in your facility’s operation center display a red screen with a ransom message demanding <insert ransom amount (e.g., $250,000)> in cryptocurrency for the decryption key and a warning that the key will expire, and all data will be sold, unless payment is received within 48 hours. The message also takes credit for the malfunctioning industrial processes, expresses gratitude for the assistance from certain employees, and threatens to continue the IT/OT system lockout.

Later that day, local news stations run stories on the ransomware attack featuring interviews with angry and concerned customers. Your organization receives requests for comment on the situation.

Discussion Questions

1. Discuss your organization’s cyber resilience planning.
   1. How are IT and OT business continuity functions coordinated?
   2. How is cybersecurity integrated into your continuity plans?
2. How does your organization baseline network activity?[[7]](#footnote-8)
   1. How do you distinguish between normal and abnormal traffic?
   2. What are your next steps when abnormal activity is detected/reported?
3. Using your organization’s cyber incident response plan (CIRP), describe the actions your organization would take to minimize impact on current operations.
   1. What guidance does the plan include to assess the severity of the incident?
   2. How does incident severity level dictate response?[[8]](#footnote-9)
   3. How are critical systems and processes incorporated within your CIRP?
4. What redundant systems exist for when primary systems are compromised?
5. What alternative systems or manual processes are implemented to continue operations if a critical system is unavailable for a significant period?
6. Does your CIRP plan include procedures to operate in manual mode if a cyber-attack compromises OT systems?
7. Who authorizes the use of alternate systems or procedures?
8. How long can you perform manual or alternate processes on your critical systems?
9. What are the roles of your network operations center/security operations center during a response?
10. Explain your organization’s decision-making process regarding ransomware payment.[[9]](#footnote-10)
    1. Are ransomware policies/procedures included in your CIRP?
    2. How are your cyber insurance provider or third-party vendors involved in your procedures?
    3. Discuss the advantages and disadvantages of either agreeing or refusing to pay.
    4. Discuss potential legal and reputational ramifications of paying or not paying the ransom.
11. How sufficient are your organization’s current internal resources for responding to the cyber incidents in this scenario?
12. What additional resources outside of your organization would be necessary for responding to the cyber incident?
13. What are the processes or procedures for requesting additional resources?
14. What external partners (e.g., CISA, FBI, EPA, etc.) would you contact for assistance?
15. Based on discussion, what changes will you implement to increase the resilience of your organization?

# Appendix A: Additional Discussion Questions

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

## Cyber Resilience

1. Discuss how cyber preparedness is integrated into your current all-hazards preparedness efforts.
2. How often are your cybersecurity plans, policies, and procedures externally reviewed or audited?
   1. What were the most recent results and action items that followed?
3. Describe your organization’s review process for your CIRP.
4. How often is the CIRP reviewed?
5. Which individual(s) and department(s) are responsible for reviewing and updating the plan?
6. How are updates to the plan communicated to relevant employees?
7. Discuss your supply chain concerns related to cybersecurity infrastructure.
8. Discuss your risk management strategy.
   1. How is it developed/maintained?
   2. Does your organization apply Zero Trust Architecture (ZTA)/zero-trust concepts?[[10]](#footnote-11)
   3. What considerations are addressed in your risk management strategy (e.g., extended downtime, impaired functionality, loss of data, etc.)?
9. What cybersecurity language is included within third-party vendor contracts?
10. How do you evaluate the cybersecurity posture of your vendors?
11. How often are contracts reviewed?
12. How do your service level agreements address cyber incident notification?
13. What level of access do your third-party vendors have to your organization’s network?
    1. What mechanisms or processes are in place to prevent malicious activity?
14. Describe your patch and vulnerability management plan.
15. What risk assessments are performed on network servers?
16. What processes are in place to proactively evaluate each server’s criticality and applicability to software patches?
17. What considerations are addressed in the plan’s risk management strategy (e.g., extended downtime, loss of data, impaired functionality, etc.)?
18. What is your method for tracking and identifying firmware vulnerabilities in your network?
19. How are IT and business continuity functions coordinated with physical security?
20. What processes do you have to ensure that your external dependencies (e.g., contractors, power, water, etc.) are integrated into your security and continuity planning programs?
21. How is the integrity of your critical data protected and validated?
22. What external entities have access to the database?
23. How do those entities report a breach of their systems to your office?
24. What essential functions are impacted by the incidents described in the scenario?
25. How does your organization maintain availability of key assets (e.g., network connectivity, etc.)?
26. If primary communications are compromised, how do you provide information to internal and external entities?
27. What policies and procedures does your organization use to decide when and how to restore backed-up data?
    1. How does your organization incorporate measures for ensuring the integrity of backup data before restoration?

## Accounts & Privileges

1. Describe your organization’s employee off-boarding process.
2. Is this process coordinated with IT and HR?
3. What additional actions are taken if the employee’s termination is contentious?
4. How 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?
5. What are your organization’s policies or procedures for IT account management?
6. What are the protocols for establishing, activating, modifying, disabling, and removing accounts?

## Incident Identification

1. How are cyber incidents reported within your organization?
2. What would trigger the reporting requirements established by regulation, law, and/or organization policy?
3. What training have employees received regarding reporting requirements and your CIRP?
4. What cybersecurity incident escalation criteria are defined in your CIRP?
5. Who is responsible and what actions would they take based on the scenario?
6. Who needs to be notified internally and externally according to the plan?
7. When is leadership notified?
8. Discuss your organization’s intrusion detection capabilities and analytics that alert you to a potential cyber incident.
9. What type of hardware and/or software does your organization use to detect and prevent malicious activity on your systems/network?
10. How often is your organization’s data reviewed?
11. How would you determine whether unauthorized manipulation of data has occurred?

## Incident Response

1. What are your processes for collecting evidence and maintaining the chain of custody during a cyber incident?
2. At what point in the scenario would you contact law enforcement?
3. How would a law enforcement investigation impact containment, eradication, and recovery efforts?
4. At what point would you notify the Environmental Protection Agency (EPA) and CISA?
5. What are the processes for contacting critical personnel outside of core hours?
6. How do you proceed if critical personnel are unreachable or unavailable?
7. How would a breach of <vendor(s)> affect your organization if they potentially have access to your information?
8. What are the notification requirements to your organization for breaches?
9. Who is responsible for coordinating information across different organizational-level incidents?

## Recovery

1. When does your organization determine a cyber incident is over?
2. Who makes this decision?
3. What post-incident activities would your organization conduct?
4. What actions would your organization take if your IT/incident response staff could not confirm the integrity of your systems/data?
5. What is the risk associated with re-activating critical business processes and systems?
6. How long and costly is the process to completely rebuild these systems?
7. What factors do you consider when making these decisions?

## Training & Exercises

1. What training does your cybersecurity incident response team undergo to detect, analyze, and report malicious activity?
   1. What additional training and/or exercise requirements do you require for your incident response staff?
2. How often does your organization exercise its CIRP?
3. Who is involved in the exercise?
4. How do your organization’s training and exercise efforts address both physical and cyber risks?
5. How often do senior staff/leadership participate in cybersecurity exercises?

## Senior Leaders

1. As a leader in your organization, what cybersecurity resilience goals have you set?
   1. How do these goals align with organizational objectives?
2. What cybersecurity training is required for senior leadership?
3. At what point would you activate your organization’s Emergency Operations Center?
4. What is your role during a cyber incident?
5. What information do you need to support your decision-making process?
6. What are the gaps in your cybersecurity workforce?
7. How does your organization recruit, develop, and retain cybersecurity staff?

## Public Information

* + - 1. What information are you sharing internally (e.g., employees, leadership)?
      2. What information are you sharing externally (e.g., residents, customers, vendors)?
      3. What training is provided to employees regarding reporting contact with the media?
      4. How do you build and maintain trust with your customers?

## Legal

1. What is the role of the legal department during a cyber incident?
2. What are the potential legal issues based on the scenario?
3. What legal documentation should your organization have for cyber incidents?

# Appendix B: Acronyms

|  |  |
| --- | --- |
| Acronym | Definition |
| CIRP | Cyber Incident Response Plan |
| CISA | Cybersecurity and Infrastructure Security Agency |
| CPG | Cybersecurity Performance Goals |
| CSF | Cybersecurity Function |
| BYOD | Bring Your Own Device |
| DDoS | Distributed Denial of Service |
| DHS | U.S. Department of Homeland Security |
| EPA | Environmental Protection Agency |
| FBI | Federal Bureau of Investigation |
| HR | Human Resources |
| ICS | Industrial Control Systems |
| IP | Internet Protocol |
| IT | Information Technology |
| KEV | Known Exploited Vulnerabilities |
| MFA | Multi-Factor Authentication |
| NIST | National Institute of Standards and Technology |
| OT | Operational Technology |
| PII | Personally Identifiable Information |
| SCADA | Supervisory Control and Data Acquisition |
| TLP | Traffic Light Protocol |
| WaterISAC | Water Information Sharing and Analysis Center |
| ZTA | Zero Trust Architecture |

# Appendix C: Case Studies

Attackers Gain Remote Access to Wastewater System Due to Vulnerability

In July 2022, a hacker group gained remote access to an Israeli town’s sewage pump control system. The system was exposed on the internet, without basic online protection such as password security or the use of Hypertext Transfer Protocol Secure (HTTPS) security. The hackers shared a screenshot of the graphic interface to confirm intrusion into the system.[[11]](#footnote-12) Local authorities initially downplayed the threat, stating that the interface was for monitoring purposes only, however experts warned that hackers could manipulate the system to potentially cause critical operational damages. The system’s exposure continued for several hours after authorities were alerted, but the municipality eventually restricted access. Researchers found that even after the attack the town’s system remained unsecure, using an outdated software version with known vulnerabilities.[[12]](#footnote-13)

## 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 the 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.[[13]](#footnote-14),[[14]](#footnote-15)

## EPA Water Sector Cybersecurity Success Stories

* <https://www.epa.gov/waterresilience/cybersecurity-planning>

# Appendix D: 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. Ransomware and associated data breach incidents can severely impact business processes, leaving organizations unable to access data necessary to function. The economic and reputational impacts of ransomware and data extortion can be challenging and costly for organizations of all sizes throughout the initial disruption and, at times, extended recovery. 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 Stop Ransomware Website (<https://www.cisa.gov/stopransomware>)
* CISA Stop Ransomware Guide

(<https://www.cisa.gov/resources-tools/resources/stopransomware-guide>)

* Protecting Against Ransomware

(<https://www.cisa.gov/news-events/news/protecting-against-ransomware>)

## Social Engineering and Phishing

One of the most prominent tactics attackers use to exploit network and system vulnerabilities is social engineering, which is the manipulation of users through human interaction and the formation of trust and confidence to compromise proprietary information. Phishing, i.e., email or malicious websites that solicit personal information by posing as a trustworthy source, is a form of social engineering. Social engineering is effective for breaching networks and evading intrusion detection systems without leaving a log trail, and it 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 involvement of human emotions. Organizations should take steps towards strengthening employee cybersecurity awareness training by incorporating trainings on identifying suspicious emails, instructing personnel on how to report them, and emphasizing the importance of keeping software systems up to date.

### Additional Resources

* Avoiding Social Engineering and Phishing Attacks

(<https://www.cisa.gov/news-events/news/avoiding-social-engineering-and-phishing-attacks>)

* Phishing Guidance: Stopping the Attack Cycle at Phase One (<https://www.cisa.gov/resources-tools/resources/phishing-guidance-stopping-attack-cycle-phase-one>)

# Appendix E: Contacts and Resources

Federal Government Contacts

* CISA (contact: [central@cisa.gov](mailto:central@cisa.gov),

<https://cisa.gov/about/contactus#:~:text=Organizations%20should%20report%20anomalous%20cyber,(888)%20282%2D0870>.)

* EPA (contact: [WICRD-outreach@epa.gov](mailto:WICRD-outreach@epa.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](http://www.ic3.gov/))
* National Cyber Investigative Joint Task Force (NCIJTF) CyWatch 24/7 Command Center (contact: [cywatch@ic.fbi.gov](mailto:cywatch@ic.fbi.gov); 855-292-3937)
* United States Secret Service (USSS) Field Offices and Electronic Crimes Task Forces (ECTFs) (contact: <https://www.secretservice.gov/contact/field-offices>, <https://www.secretservice.gov/investigation/cyber>)

State Level Resources

* Water and Wastewater Agency Response Networks

(<https://www.epa.gov/waterutilityresponse/mutual-aid-and-assistance-drinking-water-and-wastewater-utilities>)

* Multi-State Information Sharing and Analysis Center (MS-ISAC) (contact: [info@msisac.org](mailto:info@msisac.org); 518-266-3460)
* National Governors Association (NGA) (<https://www.nga.org/>)
* NGA Center for Best Practices (<https://www.nga.org/bestpractices/divisions/hsps/>)
* DHS Fusion Centers (<https://www.dhs.gov/state-and-major-urban-area-fusion-centers>)
* National Association of State Chief Information Officers (NASCIO) (<https://www.nascio.org/>)

Water Sector Resources

* EPA Cybersecurity for the Water Sector (<https://www.epa.gov/waterresilience/epa-cybersecurity-water-sector>)
  + Tabletop Exercise Tool Cybersecurity Scenario (<https://www.epa.gov/waterresilience/epa-cybersecurity-water-sector>)
  + Water Sector Incident Action Checklist

(<https://www.epa.gov/sites/default/files/2017-11/documents/171013-incidentactionchecklist-cybersecurity_form_508c.pdf>)

* CISA Water and Wastewater Cybersecurity (<https://www.cisa.gov/water>)
* CISA Industrial Control Systems (<https://www.cisa.gov/topics/industrial-control-systems>)
* Water Information Sharing and Analysis Center (<https://www.waterisac.org/>)
  + Cybersecurity Fundamentals for Water and Wastewater Utilities

(<https://www.waterisac.org/system/files/articles/15%20Cybersecurity%20Fundamentals%20%28WaterISAC%29.pdf>)

Additional Resources

* InfraGard (<https://www.infragard.org/Files/InfraGard_Redesign_2-24-2022.pdf>)
* Internet Security Alliance (<https://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](http://www.certifiedisao.org/); contact: [operations@certifiedisao.org](mailto:operations@certifiedisao.org))
* National Council of ISACs ([https://www.nationalisacs.org](https://www.nationalisacs.org/))

1. “Computer Security Resource Center Glossary: Cyber Resilience,” National Institute of Standards and Technology, accessed August 2, 2023, <https://csrc.nist.gov/glossary/term/cyber_resiliency>. [↑](#footnote-ref-2)
2. CISA, “Cybersecurity Alerts and Advisories,” <https://www.cisa.gov/news-events/cybersecurity-advisories> [↑](#footnote-ref-3)
3. CISA CPG Checklist, “2.M – Email Security,” <https://www.cisa.gov/resources-tools/resources/cisa-cpg-checklist> [↑](#footnote-ref-4)
4. CISA CPG Checklist, “2.I – Basic Cybersecurity Training,” <https://www.cisa.gov/resources-tools/resources/cisa-cpg-checklist> [↑](#footnote-ref-5)
5. CISA CPG Checklist, “2.L – Secure Sensitive Data,” <https://www.cisa.gov/resources-tools/resources/cisa-cpg-checklist> [↑](#footnote-ref-6)
6. CISA CPG Checklist, “2.S – Incident Response (IR) Plans,” <https://www.cisa.gov/resources-tools/resources/cisa-cpg-checklist> [↑](#footnote-ref-7)
7. [↑](#footnote-ref-8)
8. CISA CPG Checklist, ”2.S Incident Response (IR) Plans,” <https://www.cisa.gov/resources-tools/resources/cisa-cpg-checklist> [↑](#footnote-ref-9)
9. CISA, “Stop Ransomware,” <https://www.cisa.gov/stopransomware> [↑](#footnote-ref-10)
10. CISA Resources, “Zero Trust Maturity Model,” <https://www.cisa.gov/zero-trust-maturity-model> [↑](#footnote-ref-11)
11. “2022 Cyberattacks on Operational Environments: What They Mean for 2023,” *Otorio*, December 14, 2022, <https://www.otorio.com/blog/2022-cyberattacks-critical-infrastructure-industrial-manufacturing/>. [↑](#footnote-ref-12)
12. Oded Yaron, “Cyber Sewage Attack? Hackers Show How Easy It Is to Flood Israel,” *Haaretz*, July 10, 2022, <https://www.haaretz.com/israel-news/security-aviation/2022-07-10/ty-article/.premium/cyber-sewage-attack-hackers-show-how-easy-it-is-to-flood-israel/00000181-e836-dd94-a5b3-fdf69f170000>. [↑](#footnote-ref-13)
13. Kevin Collier, “A Hacker Tried to Poison a California Water Supply,” *NBC News,* June 17, 2021, <https://www.nbcnews.com/tech/security/hacker-tried-poison-calif-water-supply-was-easy-entering-password-rcna1206>. [↑](#footnote-ref-14)
14. James Crump, “Hackers Tried to Poison California Water Supply in Major Cyber Attack,” June 18, 2021, *Newsweek,* <https://www.newsweek.com/san-francisco-water-plant-hack-cyber-attack-poison-supply-1601798>. [↑](#footnote-ref-15)