Cyber Readiness
Playbook Guide

Water Utility Addendum

Special Companion to the
Cyber Readiness Program
for the Cyber Leader in a
Water or Wastewater Utility

CYBER READINESS
INSTITUTE

Table of Contents

Introduction and Purpose

Introduction

First, thank you for serving as the Cyber Leader in your water or wastewater utility and dedicating your time to completing the Cyber Readiness Program. Your efforts will strengthen your utility's ability to reduce the risk of cyber incidents and improve its response when an incident occurs. As the Cyber Leader, you play a crucial role in achieving this goal.

This Water Utility Addendum is a supplement to the online Cyber Readiness Program and the Cyber Readiness Playbook Guide and Playbook. While it equally applies to water and wastewater systems, we will broadly refer to both as water utilities.

This document provides additional guidance for Cyber Leaders at water utilities to address the unique cybersecurity challenges of your operational technology (OT) that controls your facility and the information technology (IT) that you use for business purposes such as email and billing.

This Addendum is not intended to replace the Playbook Guide, so we have tried to minimize any duplication.

The goal remains for you to build a culture of cyber readiness in your water utility by completing the Cyber Readiness Playbook. The Playbook will help you prioritize what data, OT systems, and IT systems that are most important to your operations. It includes policies you can use or adapt, based on what the Cyber Readiness Institute and its member companies have identified as four key aspects of cyber readiness. It includes a Business Continuity Plan template, so you can document what to do and who to call if something happens. Think of the Business Continuity Plan as a cyber component of your U.S. Environmental Protection Agency (EPA) or state-required Emergency Response Plan. Finally, it includes a form for you to attest that everyone in your water utility has been trained on the basics of cyber readiness.

Thank you again for your participation in the Cyber Readiness Program. You can make a difference in your water utility and your community by taking practical steps to be cyber ready. Be cyber ready. Be cyber strong.

How to Use This Addendum

We have designed this Addendum to follow the same structure as the Playbook Guide and Playbook so you can easily use it as a reference when you are developing and maintaining your Playbook. The Addendum provides specific information and guidance relevant to your water utility. It minimizes duplication of the information in the Playbook Guide.

How Water Utilities Can Use the Cyber Readiness Playbook

The Playbook contains policies, forms, and checklists aligned with the Cyber Readiness Program for you to use. It is designed as a living document to help you build a culture of cyber readiness in your water utility.

As you complete the Playbook, it is important for you to think about all the OT and IT used in your operations. This may include the hardware and software used for:

- SCADA (Supervisory Control and Data Acquisition) systems
- Control systems
- Programmable logic controllers and remote terminal units
- Alarm notification
- Security cameras
- Metering
- Remote access
- Billing and payment processing
- OT data communications
- IT business communications
- Geographical Information Systems (GIS) for field asset mapping
- Work orders

Cyber Readiness Program Overview for Water Utilities

As part of critical infrastructure, water utilities are increasingly targeted by hackers. This makes being cyber ready more critical than ever. Malicious cyber attackers exploit common habits and predictable behaviors to get past even the most advanced security technologies. That's why the Cyber Readiness Institute has developed a program focused specifically on human behavior.

For water utilities, the challenge is greater because of the interaction between Operational Technology (OT) systems and Information Technology (IT) systems. Your critical role in the health and safety of your community makes your success essential.

Water Utilities Under Attack

11

There were 11 publicly reported cyberattacks on water and wastewater plants in the prior two years, according to a report published by Wisdiam on October 13, 2024. Most cyberattacks on water utilities are not publicly reported.

62%

Semperis released a study on April 3, 2025, analyzing cyberattacks targeting water and electricity operators across the U.S. and U.K. **In the past year, 62% of utility operators were targeted by cyberattacks.**

Role of Cyber Leader at a Water Utility

Water utilities have unique cybersecurity challenges due to the need to protect the various OT and IT systems. Your IT system may be part of the town or county IT system. IT support may be provided by a municipal employee or by a contractor. It is likely that you have completely different OT systems for water and wastewater with the support provided by different vendors. All these factors make it more challenging to build a culture of cyber readiness.

However, given the critical importance of your water utility to your community, your commitment is more important than ever.

Look at the Playbook Guide for more details on your role and how to excel as a Cyber Leader. You do not need to be a cybersecurity expert. At many utilities the Superintendent takes on the role for both IT and OT cybersecurity. Sometimes there is a division of responsibility, where for instance a community's IT department takes on the role of the IT Cyber Leader and the Superintendent or other management level person in the utility's operations department takes on the OT Cyber Leader role. If that is the case, there needs to be close and regular collaboration between the two individuals.

The Core Four for Water Utilities

The Cyber Readiness Program is focused on four basic cyber hygiene activities we call the "Core Four." Adopting and implementing CRI's Core Four policies will greatly reduce your risk of a cyber incident and shift you from being reactive to being proactive and preventative. Implementing the Core Four policies will not cost you any money because they focus on taking practical steps to change human behavior.

THE CORE FOUR

1. 

Passwords + Multifactor Authentication

2. 
Software Updates

3. 
Phishing

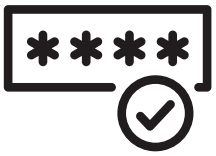
4. 
Secure Sharing and Storage

Special Considerations for Using the CRI Core Four Policies at Water Utilities

In the Playbook, there is a policy template to use for your water utility's cyber policies. The Playbook Guide has general details on the Core Four policies.

Protecting your OT systems and ensuring the delivery of water or wastewater service is the most important end goal. Hackers will try to gain access to your OT systems through the weakest link in your software and firmware. This could be through your IT system, your remote access, or even your alarm software. Once in the OT system, Hackers can easily disrupt your ability to provide safe clean water and properly process wastewater while disabling any alarms and falsifying system status.

1 Passwords+ for Water Utilities



The first line of defense against opportunistic hackers is strong authentication, consisting of 15-character or longer passwords and the use of multifactor authentication (MFA).

List all the IT and OT software, hardware, and systems used to operate your water and wastewater operations, using the "Comprehensive Software Listing" and "Comprehensive Hardware Listing" sheets in the Cyber Readiness Playbook. Don't forget about:

- SCADA system computers and software
- Programmable logic controllers and remote terminal units
- Alarm and notification software
- Metering and billing software
- Security cameras
- Devices used in the field
- Remote access equipment and software
- Network communications equipment (i.e., internet routers)
- Network segmentation and other cybersecurity equipment and software
- Personal and business owned devices that may be used for remote access or OT maintenance

Then list all the people that access each piece of software or hardware. Be sure to include:

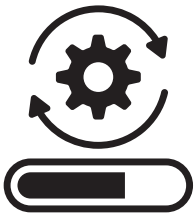
- Employees working at the water utility
- Contractors working at the water utility
- Employees or contractors in other departments of the town or county
- Vendors or consultants for any of the OT systems
- Vendors or consultants for any of the IT systems

Combine these lists to create one checklist to use for overseeing who has access and to make sure they are using 15-character or longer passwords and MFA. The information you collect here will make completing the Software Update Management Tool faster and easier.

> **Change the default passwords on all OT and IT devices.** Require all users to use MFA on every system that offers it. Look to upgrade remote access systems and other internet exposed systems that do not have an MFA option.

For more details, check out the Playbook Guide.

2 Software Updates



Many cyberattacks target systems using software with known weaknesses or vulnerabilities. Hackers know that people are often slow to update their software, and they take advantage of this.

In addition to updating software automatically, water utilities also need to update equipment firmware and hardware. Firmware is the code that lets software interact with hardware. It is in computers, controllers, firewalls, routers, and other equipment. Firmware also has vulnerabilities that adversaries target. Finally, hardware needs to be upgraded before it reaches its end-of-life and is no longer supported with software and firmware security updates by the manufacturer.

It is important to keep all your software, firmware, and hardware up to date. It is a critical priority to update the parts of your OT system that are externally exposed to the Internet or to your IT system, which can be used by hackers as an attack path. Examples of exposed components that need priority updating include remote access software, alarm notification software, and firewall firmware.

> **Make sure that there is absolute clarity about who is responsible** for maintaining software, firmware, and hardware updates in each OT and IT system. This can be complicated because there can be several parties involved.

For more details and for the Software Update Management Tool, check out the Playbook Guide.

3 Phishing

Phishing uses deceptive messages to gain access to your OT systems, IT systems, and data through an individual user. Any person with an email account or smartphone can put your organization at risk by clicking on links in phishing messages.

For water utilities you need to make sure that everybody that has access to your OT and IT systems and any supporting systems is aware of the danger and knows how to spot phishing attempts. This includes your employees, municipal employees in other departments, IT consultant or MSP, OT integrator, and vendors.

> **Hackers are using Generative AI** to create more frequent and more convincing deceptive emails, texts, and other messages to fool your users. They will hijack a real email address and send fake messages to attempt a Business Email Compromise (BEC) attack that redirects the electronic transfer of funds to the hacker. Frequent communications to your workforce are critical to building awareness. Tell people if they have any suspicion to call the person directly.

For more details, check out the Playbook Guide.

4 Secure Storage and Sharing

The connection and transfer of data between your OT and IT systems creates a cyber risk for water utilities.

The first step is to understand and map the flow and storage of data between your OT and IT systems. This may be completely different for your water and wastewater systems. Transferring data between systems using USBs and other removable media creates a cyber risk that needs to be managed.

Remote access is an area hackers will target. It is critical that you know who is responsible for managing each aspect of your IT and OT systems. If the remote access to your OT and IT systems is done through your municipal IT system, you will need to coordinate with them.

Mapping the data flow will help you understand the cyber risk and determine the optimal degree of network segmentation or isolation. You want to make it easy and efficient for necessary data to flow between the systems but make it difficult for a hacker to move into your OT systems if they have penetrated your IT system.

Although your goal is to prevent attacks, you must be prepared for a successful attack. This is where backups come into play. OT backups of important documentation may include SCADA software, PLC programs, HMI configuration files, communication equipment settings and rules, license information, a record of standard set points, and even hardware spares in case attacked equipment becomes unusable. OT backups typically occur when changes are made to the OT system, as compared to the regular and frequent updates made on the IT side.

> **OT and IT systems will need to have separate backups for each system.** You may also need separate backups for water SCADA systems and wastewater control systems. Clearly define who is responsible for doing and testing the backups. Be sure to keep at least one copy off-line where it cannot be corrupted during an attack.

For more details, check out the Playbook Guide.

Business Continuity Plan

A Business Continuity Plan outlines what you need to do to continue the delivery of water and the treatment of wastewater during an incident and how to minimize the disruption. This is very similar to the Emergency Response Plan (ERP) that is required by the EPA and state regulatory agencies.

For water utilities, make sure that your business continuity plan includes natural and environmental disasters, operational risks, public health risks, and cybersecurity risks. As part of this, be prepared for the manual operation of water and wastewater systems if your OT systems are down.

For more details, check out the Playbook Guide.

Prioritization Worksheet for Water Utilities

The Prioritization Worksheet in the Playbook is used to list the data, software, and hardware you use to operate. As we have repeated throughout this Addendum, it is critical that you consider all OT and IT systems that impact your operations.

Start by listing everything you can think of — the more detail the better. This list will be useful as you complete the Software Update Management Tool in the Playbook.

The next step is to prioritize what is most important to your mission of providing water and treating wastewater. You can't protect everything equally well, so it is critical to know what is most important.

As you prioritize, ask yourself and others in your utility, especially senior management and operations staff, these questions:

1. **What data would be the most damaging for us to lose, go public or not be able to access?**
   a. Operational data (e.g., consumption, pressure, flow rates)
   b. Infrastructure data (e.g., asset locations, maintenance history and schedule)
   c. Compliance and quality data (e.g., water quality test results, compliance with water and wastewater standards)
   d. Financial data (e.g., billing, collections)

2. **What software would cause the most damage to our ability to operate if it went down? Consider all aspects of your OT and IT operations.**
   a. SCADA and control system software
   b. Alarm software
   c. Remote access software
   d. Meter reading software
   e. GIS software
   f. Billing software
   g. Work order software
   h. Software for communicating with employees, customers or suppliers (like email or websites)
   i. Software for creating documents, presentations, graphics, reports

3. **What hardware devices would cause the most damage to our ability to operate if they went down?**
   a. Programmable logic controllers and remote terminal units
   b. Network communication equipment
   c. Data radios
   d. Variable frequency drives
   e. Skid systems
   f. Pump controllers
   g. Automatic transfer switches
   h. Desktop or laptop computers used for the control system
   i. Tablets or smartphones
   j. Printers

For more details, check out the Playbook Guide.

Incident Response Plan

The Incident Response Plan is used to identify your Emergency Contacts and list the steps needed to prepare for, respond to, and recover from a cyber incident. For water utilities, the cyber incident response plan is a critical component of your overall business continuity plan. Your plan needs to cover when and how to go to manual operations if needed. You should train your workforce on the plan, so everyone knows what they need to do at each step.

Prepare

The time you invest in preparation will pay enormous dividends. The Core Four is intended to help you prevent incidents, but all it takes is the exploitation of a previously unknown vulnerability or one mistake by one person, and you've got a cyber incident.

For water utilities it is essential that your preparation covers all OT and IT systems. There may be different emergency contacts if it's a breach of the OT system or the IT system. Important contacts not listed in the Playbook include your state regulator, your cyber insurance company, your operations lead, senior management, the FBI, and possibly CISA.

Maintaining current backups is critical to good preparation. Network segmentation is important, so you can isolate a breach from spreading. It is good practice to conduct incident response tests with your team. This allows you to train them how to quickly shift to manual operation, or how to react if a pump shuts off, or alarms fail to indicate a surge in water pressure.

Respond

As the Cyber Leader for your water utility, you should be the first person notified of a suspicious event or a cyber incident. If your utility has both an OT Cyber Leader and an IT Cyber Leader, make sure both individuals are participating in the respond.

This part of the plan describes what steps to take based on what OT and IT systems are impacted. Initial actions might include disconnecting a compromised device from the control network, isolating the control network from the IT network and the internet, and possibly disabling the control system and shifting to manual operations, The steps need to be identified and only implemented with the input and approval of operations staff to prevent unintended consequences.

Contact all relevant people on your Emergency Contact list, starting with the primary contacts for the breached system and then moving down the entire list, so everyone is informed.

Recover

The better the preparation, the easier the recovery. This is when you are thankful for current software and configuration backups, and spare hardware. The specifics of the recovery will depend on which OT and IT systems were impacted and a detailed understanding of the extent of the attack.

For more details, and for an Incident Response Plan template, check out the Playbook Guide.

Software Update Management Tool

One of the Core Four policy requirements is maintaining the Software Update Management Tool. As you know by now, keeping all the software, firmware and hardware used in your water utility updated is a key part of being cyber ready. To this end you may want to modify or append the tool to include hardware model, end-of-life date, and firmware and software versions. The Tool includes a column for "Auto-Update Enabled." Auto-updating may be appropriate for IT systems but is generally not recommended for OT systems.

In the Playbook, we intentionally put this Tool after the Prioritization Worksheet because you should refer to your Prioritization Worksheet when you fill out the Software Update Management Tool. It is important to include all the OT and IT software used in every system. Refer to the lists you developed for Password + MFA as a source.

For water utilities, we recommend including firmware in the Software Update Management Tool. The more detail the better.

For more details, and for a Software Update Management Tool template, check out the Playbook Guide.

Training and Communication

Making your water utility cyber ready involves changing human behavior. Every person that touches your OT and IT systems needs to take basic steps to reduce your cyber risk. Changing behavior requires more than annual training sessions. It requires short, frequent communications that maintain the awareness of cyber readiness and reinforce what to do. Consider thinking about this in the same way you approach safety, with a "cybersecurity minute".

To accelerate your training and communication program, you can access and share CRI's short videos on the Core Four and Business Continuity. PowerPoint templates, email templates, and posters are also available to support you.

For more details on CRI training and communication resources, check out the Playbook Guide. The Playbook Guide also includes links to additional resources published by CRI and other leading organizations. Useful resources specifically for water utilities include:

- EPA Cybersecurity for the Water Sector
- WaterISAC
- AWWA

Celebrating and Sustaining Your Success

Cyber readiness is a journey, not a destination. Hackers are targeting water utilities with more sophisticated attacks. The complexity of the interrelationship between your OT and IT systems requires everyone to be diligent.

However, it is important to pause on the journey to recognize your effort and that of your team. It's unfortunate, but true, that those that prevent a horrible incident don't get enough recognition. Make a point of congratulating everyone on the positive impact you have on your community.

For tips on sustaining cyber readiness, check out the Playbook Guide.

CYBER READINESS
INSTITUTE

cyberreadinessinstitute.org