



EPA Water Sector Cybersecurity Overview

About Me

- **Cole Dutton, Cybersecurity Specialist**
- **EPA's Office of Water – Water Infrastructure and Cyber Resilience Division**
- **M.S – Computer Science, Information Security**





Overview of Cybersecurity Threats to Water and Wastewater Systems

Cyber Threats to Water and Wastewater Systems

- **Disabling or contaminating the drinking water to consumers and other essential facilities**
- **Ransomware and other malicious malware which can disable business enterprise and/or process control operations**
- **Unauthorized exposure of customer and employee personal identifiable information (PII)**



Information Technology vs Operational Technology

Information Technology (IT)

- Manages data and information used to support business operations (billing, payroll, etc.)

Operational Technology (OT)

- Hardware and software that detects or causes a change through the direct monitoring or control of physical devices, processes, and events in the enterprise

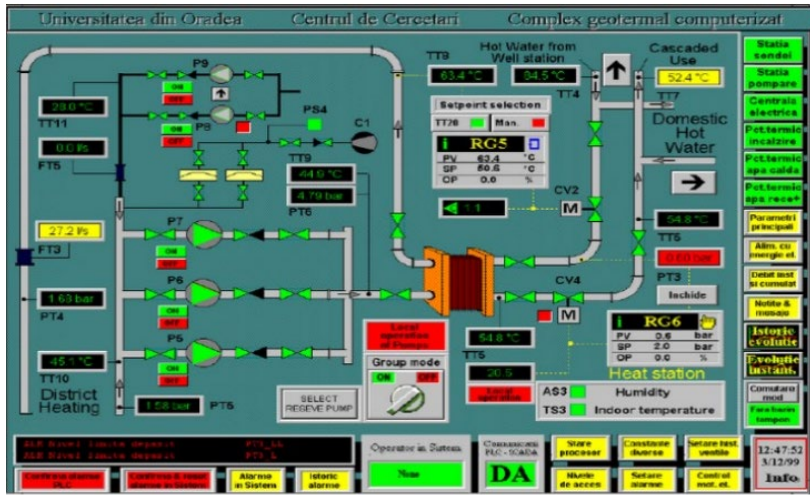


Figure 1 SCADA



Figure 2 HMI

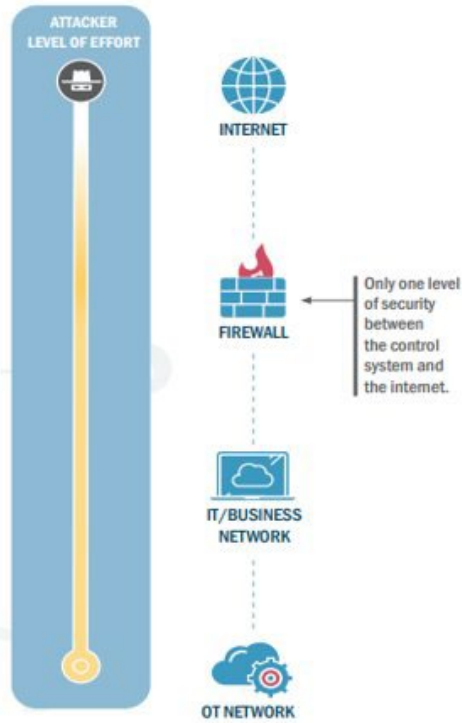


Figure 3 PLC



Figure 4 RTU

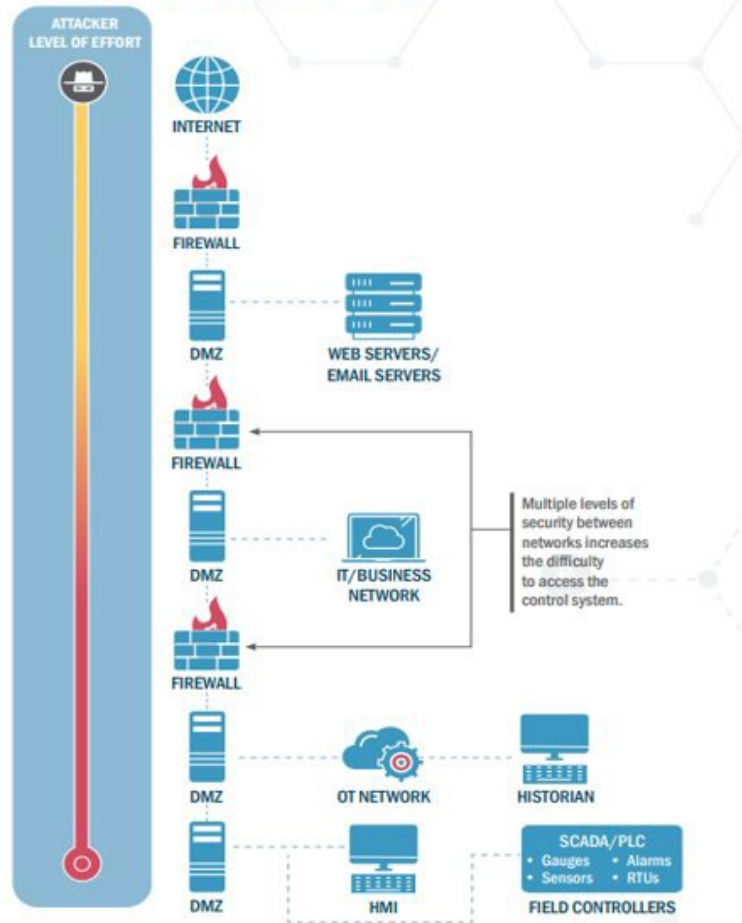
FIGURE 1: UNSEGMENTED IT AND OT NETWORK



UNSEGMENTED IT AND OT NETWORKS INCREASE RISK²:

- OT networks are exposed to vulnerabilities in connected IT networks.
- Easier for threat actors to move laterally after breaching the IT network.
- Detecting threat actors is more difficult due to increased volume of network traffic.

FIGURE 2: A SEGMENTED PURDUE ENTERPRISE REFERENCE ARCHITECTURE (PERA) NETWORK ARCHITECTURE



BENEFITS OF SEGMENTING BETWEEN IT AND OT NETWORKS:

- Segmented zones isolate and protect high-value assets and data.
- Malicious traffic is easier to detect, prevent, and contain.
- Threat actors must negotiate multiple firewalls and other protocols to access the OT environment.

California Water Treatment Facility

CYBERCRIME

Former Contractor Employee Charged for Hacking California Water Treatment Facility

Former contractor employee charged with hacking for accessing the systems of a water treatment facility in California to delete critical software.

- **Employee resigned in January 2021, used remote access software to enter the water facility's systems**
- **The employee successfully uninstalled software that protected the entire water treatment system including water pressure, filtration, and chemical levels**

Kansas Drinking Water Utility

- Former employee's remote login credentials were not revoked when they departed the utility
- The former employee used the unrevoked login credentials to shut down the plant, along with one of its treatment filters

LOCAL NEWS

Kansas hacker pleads guilty to shutting down drinking water plant with phone

by: [Mark Feuerborn](#)

Posted: Oct 21, 2021 / 06:03 PM CDT

Updated: Oct 21, 2021 / 06:03 PM CDT

"There is no doubt that Travnichek's intentional actions directly placed the public in harm's way. The plea should send a clear message to anyone who attempts to tamper with public facilities."

- CHARLES DAYOUB, FBI SPECIAL AGENT

Maine Rural Wastewater Utility

- **Attackers compromised an obsolete Windows 7 computer that was used as a control computer for the treatment system**
- **All files on the computer were encrypted and important safety alarms were taken offline**
- **The treatment system had to be operated in manual mode until the control computer was replaced**

Rural sewage plants hit by ransomware attacks in Limestone



Cybersecurity Program Case Study of a Small Wastewater System

Overview

All mechanical operations became automated when a new wastewater treatment plant came online in 2017. The plant operator had to balance the welcomed convenience of automation and productivity with the new cybersecurity risks introduced

Action Taken

The utility developed a cybersecurity policy document to ensure that vulnerabilities were considered, and cybersecurity risks mitigated

Topics Covered in the Utility's Cybersecurity Policy Document

Account Security	Device Security	Data Security
<ul style="list-style-type: none"> • Separate standard user and privileged accounts • Password length requirements • Secure remote access policy 	<ul style="list-style-type: none"> • OT and IT network asset inventory 	<ul style="list-style-type: none"> • Log collection and monitoring frequency for intrusion detection
Vulnerability Management	Response and Recovery	Other
<ul style="list-style-type: none"> • OT asset connections to the public internet 	<ul style="list-style-type: none"> • Cybersecurity incident reporting • Cybersecurity Incident Response Plan for incidents such as disabled process control systems • System backups 	<ul style="list-style-type: none"> • Segmentation of OT and IT networks



EPA Cybersecurity Resources for Water and Wastewater Utilities



Free EPA Cybersecurity Assessment Resources

Self-Assessment


Checklist and Water
Cybersecurity Assessment Tool
(WCAT)

Third-Party Assessment

Water Sector Cybersecurity
Evaluation Program

Water Cybersecurity Assessment Tool (WCAT)

- Utilizes EPA's Cybersecurity Checklist and provides a method to evaluate cybersecurity practices at water and wastewater utilities
- The Tool Includes:
 - Assessment Workbook
 - Assessment Report
 - Risk Mitigation Plan

EPA Water Cybersecurity Assessment Tool (WCAT) 

Please read the following instructions in their entirety prior to completing the assessment.

How to Use This Tool

- 1) Open the 'Assessment Workbook' tab. For security reasons, the information fields at the top of the page may be completed so as to avoid identifying the utility: Utility ID - create a unique identifier; Public Water System (PWS) staff - include initials for all staff participating in the assessment; Assessment Date - self explanatory; Assessor Name - identify a lead individual from an outside agency (for 3rd party assessments) or the utility (for self-assessments) who is filling out the questionnaire. Complete the questionnaire by selecting from the available dropdown options for each question ("Yes", "No", or "In Progress"). Be sure to document explanatory notes in the "Explanation of Response" column for each response.

Note: If the answer to an assessment question is unknown, please select "No" as the response. The assessment can be updated later once an appropriate response is known.
- 2) **Upon completion of the assessment, and before you move to the 'Assessment Report' tab, you must refresh the data in the tool to auto-complete the 'Assessment Report' and 'Risk Mitigation Plan' tabs.** To do this, select "Data" from the ribbon at the top of the screen in Excel and click "Refresh All". Alternatively, you may press Alt+A+R.
- 3) Now open the 'Assessment Report' tab and export/paste the Cybersecurity Assessment Report into Word. To do this, press Ctrl+A twice and then Ctrl+C. Open a blank Word document and press Ctrl+V to export/paste the report into the document. The Cybersecurity Assessment Report displays all checklist questions regardless of response. You may edit the report as needed. The report content is displayed in one Word table.
- 4) Now open the 'Risk Mitigation Plan' tab and export/paste the Cybersecurity Risk Mitigation Plan to Word. To do this, press Ctrl+A twice and then Ctrl+C. Open to a blank Word document and press Ctrl+V to export/paste into the document. The Cybersecurity Risk Mitigation Plan will only display checklist items answered "No" or "In Progress" during the assessment. You may edit the plan as needed, as questions answered "yes" will create blank rows at the end of the plan. The plan content is displayed in one Word table.

WCAT Assessment Workbook

EPA Cybersecurity Checklist

Utility ID:

W/WS Staff (Initials Only):

Assessment Date:

Assessor:



Topic	Topic Number	Checklist Number	Question	Response	Recommendation	Explanation of Response
Account Security	1.0	1.1	Does the W/WS detect and block repeated unsuccessful login attempts?		Where technically feasible, System Administrators should be notified after a specific number of consecutive, unsuccessful login attempts in a short amount of time. At that point, future login attempts by the suspicious account should be blocked for a specified time or until re-enabled by an Administrator.	
		1.2	Does the W/WS change default passwords?		When feasible, change all default manufacturer or vendor passwords before equipment or software is put into service.	
		1.3	Does the W/WS require multi-factor authentication (MFA) wherever possible, but at a minimum to remotely access W/WS Operational Technology (OT) networks?		Deploy MFA as widely as possible for both information technology (IT) and operational technology (OT) networks. At a minimum, MFA should be deployed for remote access to the OT network.	
		1.4	Does the W/WS require a minimum length for passwords?		Where feasible, implement a minimum length requirement for passwords. Implementation can be through a policy or administrative controls set in the system.	
		1.5	Does the W/WS separate user and privileged (e.g., System Administrator) accounts?		Restrict System Administrator privileges to separate user accounts for administrative actions only and evaluate administrative privileges on a recurring basis to be sure they are still needed by the individuals who have these privileges.	
		1.6	Does the W/WS require unique and separate credentials for users to access OT and IT networks?		Require a single user to have two different usernames and passwords; one set is to be used to access the IT network, and the other set is to be used to access the OT network. This reduces the risk of an attacker being able to move between both networks using a single login.	
		1.7	Does the W/WS immediately disable access to an account or network when access is no longer required due to retirement, change of role, termination, or other factors?		Take all steps necessary to terminate access to accounts or networks upon a change in an individual's status making access unnecessary.	
		2.1	Does the W/WS require approval before new software is installed or deployed?		Only allow Administrators to install new software on a W/WS-issued asset.	

Overview of EPA's Cybersecurity Checklist

Cybersecurity Control Family	# of Questions/Goals
1. Account Security	7
2. Device Security	5
3. Data Security	4
4. Governance and Training	5
5. Vulnerability Management	3
6. Supply Chain/Third Party	2
7. Response and Recovery	4
8. Other	3
Total:	33

Questions from the WCAT

- ***1.2 Does the w/ws change default passwords?***
- ***2.3 Does the w/ws maintain an updated inventory of all OT and IT network assets?***
- ***3.1 Does the w/ws collect security logs (e.g., system and network access, malware detection) to use in both incident detection and investigation?***

Questions from the WCAT

- ***4.3 Does the w/ws provide at least annual training for all utility personnel that covers basic cybersecurity concepts?***
- ***5.1 Does the w/ws patch or otherwise mitigate known vulnerabilities within the recommended timeframe?***
- ***6.2/6.3 Does the w/ws require that all OT and IT vendors and service providers notify the utility of any security incidents or vulnerabilities in a risk-informed timeframe?***

Questions from the WCAT

- ***7.2 Does the w/ws have a written cybersecurity Incident Response (IR) Plan for critical threat scenarios which is regularly practiced and updated?***
- ***8.1 Does the w/ws segment OT and IT networks and deny connections to the OT network by default unless explicitly allowed?***

WCAT Assessment Report Tab

- Provides a summary of results from the completed Cybersecurity Assessment
- This assessment report is intended to be placed in a Word Document and provided to the utility. To do this, highlight the cells on this tab, copy, and paste in a blank Word Document

Account Security			
Checklist Number	Question	Response	Explanation of Response
1.1	Does the PWS detect and block repeated unsuccessful login attempts?	Yes	
1.2	**Does the PWS change default passwords?	Yes	
1.3	**Does the PWS require multi-factor authentication (MFA) wherever possible, but at a minimum to remotely access PWS Operational Technology (OT) networks?	In Progress	
1.4	**Does the PWS require a minimum length for passwords?	No	
1.5	Does the PWS separate user and privileged (e.g., System Administrator) accounts?	No	
1.6	Does the PWS require unique and separate credentials for users to access OT and IT networks?	No	
1.7	**Does the PWS immediately disable access to an account or network when access is no longer required due to retirement, change of role, termination, or other factors?	No	

WCAT Cybersecurity Risk Mitigation Plan Template

Account Security	1.4	Question:	Does the W/WS require a minimum length for passwords?
		Planned Risk Mitigation Action:	<i>Where feasible, implement a minimum length requirement for passwords. Implementation can be through a policy or administrative controls set in the system.</i>
		Current Status:	Not Started
		Target Completion Date:	January 1st, 2024
		W/WS Personnel Responsible:	Joe Smith and Kate Ward
		Involved Departments and/or Agencies:	System Administrator
		W/WS Notes:	We will be working internally to get a procedure in place to implement this control.

EPA Water Sector Cybersecurity Evaluation Program

- This program will conduct cybersecurity assessments for water and wastewater utilities.
- Uses the EPA Checklist.
- Utilities will receive a report with response to the checklist questions that shows cybersecurity gaps.
- Link:
<https://www.epa.gov/waterriskassessment/forms/epas-water-sector-cybersecurity-evaluation-program>

EPA's Water Sector Cybersecurity Evaluation Program

Please share your information to receive more information about EPA's Water Sector Cybersecurity Evaluation Program.

Primary Contact Name *

Secondary Contact Name

Primary Contact Email Address *

Secondary Contact Email Address

Primary Contact Phone Number *

Secondary Contact Phone Number

Email addresses for all additional contacts to be included in communications (if applicable)

Cybersecurity Technical Assistance Program for the Water Sector

- Under this program, states and PWSs can submit questions or request to consult with a subject matter expert (SME) regarding cybersecurity.
- EPA will strive to have an SME respond within two business days.
- All assistance will be remote.
- Link:
<https://www.epa.gov/waterriskassessment/forms/cybersecurity-technical-assistance-water-utilities>

Water Utility Risk Assessment CONTACT US

Cybersecurity Technical Assistance Program for the Water Sector

Please share your information to request cybersecurity technical assistance.

Contact Name *

Contact Name 2 (optional)

Contact Email Address *

Contact Email Address 2 (optional)

Contact Phone Number *

Contact Phone Number 2 (optional)

Preferred Method of Contact *

Phone

Email

EPA Cybersecurity Checklist Fact Sheets

- Fact Sheets are available for each question on the EPA Checklist and include:
 - Recommendations
 - Overview of why the control is important
 - Additional Guidance
 - Implementation Tips
 - Additional Resources
 - Estimate for Cost, Impact, and Complexity

Account Security: Detection of Unsuccessful (Automated) Login Attempts

COST: \$\$\$\$ IMPACT: HIGH COMPLEXITY: LOW

1.1: Does the PWS detect and block repeated unsuccessful login attempts?

Recommendation: Where technically feasible, system administrators should be notified after a specific number of consecutive, unsuccessful login attempts in a short amount of time. At that point, future login attempts by the suspicious account should be blocked for a specified time or until re-enabled by an administrator.

Why is this control important?

A common technique that attackers use to break into OT and IT systems is to attempt to “guess” an actual username and password login combination. This can be accomplished by manually guessing an account’s password, using a list of common passwords, or through a technique called a *brute force attack*. In this type of attack, an attacker uses a trial-and-error approach to systematically guess login credentials. The attacker submits combinations of usernames and passwords, generally using an automated password-breaking tool, until the guess is correct. Blocking an attacker from future guesses after a specified number of incorrect guesses can stop these types of attacks.

Additional Guidance

- Enable systems to automatically notify (e.g., by a computer-generated alert) security teams or the system administrator after a specific number of consecutive, unsuccessful login attempts in a short time period (e.g., five failed attempts in under 2 minutes).
- Enable account lockout settings on applicable systems to prevent future login attempts for the suspicious account for a minimum time or until the account is re-enabled by the system administrator.
- It is a good practice to ensure that the account lockout duration is set to 15 minutes (or more) or to require a user with administrative privileges to unlock a user’s account.
- Log and store the alert information for analysis. Use sound logging procedures - a log should capture event source, date, username, timestamp, source addresses, destination addresses, and any other useful information that could assist in a forensic investigation.

Implementation Tips

Depending on your version of Windows, you can use the Local Security Policy to restrict the number of login attempts. To access this feature, type “Local Security Policy” in the search box in the Start menu and click on the Local Security Policy App. Once the menu pane opens, click on “Account Policies” to adjust login attempts and lockout duration.

If your PWS utilizes a Microsoft Domain where many systems and user accounts are connected to a single domain, these settings can be managed using Group Policy Objects (GPOs). The Account Lockout Policy settings can be enabled in the following location in the Group Policy Management Console: Computer Configuration\Windows Settings\Security

Cybersecurity 101 Webinar for Water Systems

This webinar reviews basic cybersecurity topics including:

- Account security
- Device security
- Data security
- Training, and more.



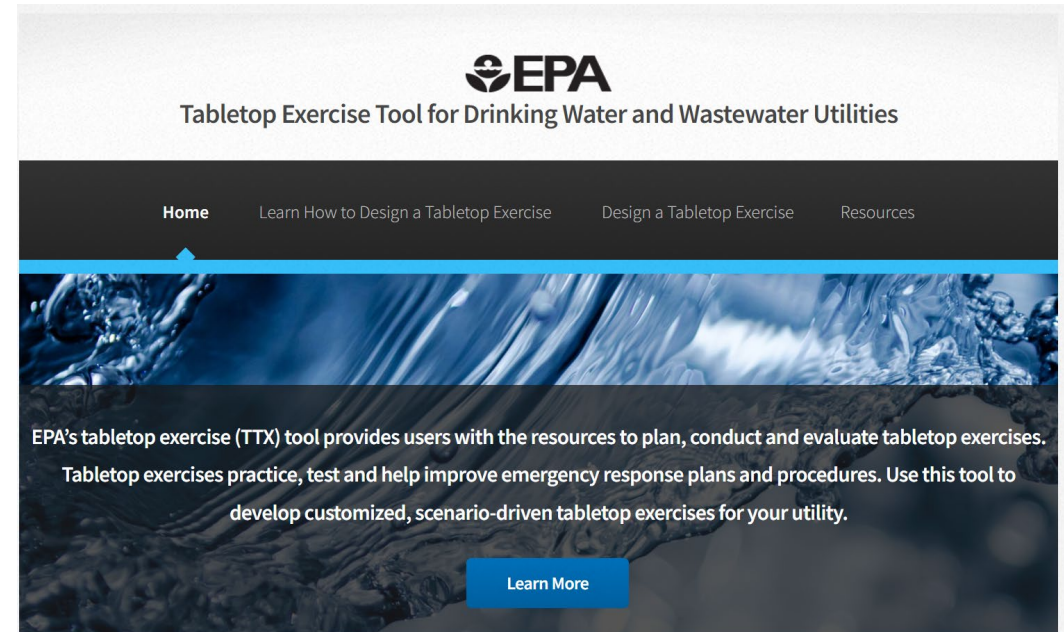
Link: <https://www.youtube.com/watch?v=e2QDbgrojb0>

EPA Tabletop Exercise Tool for Utilities

- You can download the TTX tool here:

<https://www.epa.gov/waterresiliencetraining/develop-and-conduct-water-resilience-tabletop-exercise-water-utilities>

If you are interested in having a TTX in your state, please contact us at watercyberta@epa.gov





Funding



Drinking Water State Revolving Fund

- **Projects can include cybersecurity items such as:**
 - Sensors
 - SCADA upgrade
 - Cyber assessments

Drinking Water System Infrastructure Resilience and Sustainability Program

- **Purpose:** Infrastructure funding to underserved and small (less than 10,000) or disadvantaged PWSs for the purpose of protecting water sources from natural hazards
- **Funding amount:** \$19,000,000
- **Eligibility:** PWSs in an area governed by an Indian Tribe, or States on behalf of communities, which are underserved and small or disadvantaged.
- **Application period:** **Open Now**
- [Drinking Water Infrastructure Resilience and Sustainability Grant Information \(epa.gov\)](https://www.epa.gov/dwrs)

Midsize & Large Drinking Water System Infrastructure Resilience & Sustainability Program

- **Purpose: Protecting drinking water sources from natural hazards, extreme weather events, and cybersecurity threats**
- **Funding amount: ~\$5,000,000 +**
- **Eligibility: Public water systems serving more than 10,000 people**
- **Application period: Open for applications in 2024**

Link to our Website

<https://www.epa.gov/waterriskassessment/epa-cybersecurity-best-practices-water-sector>

