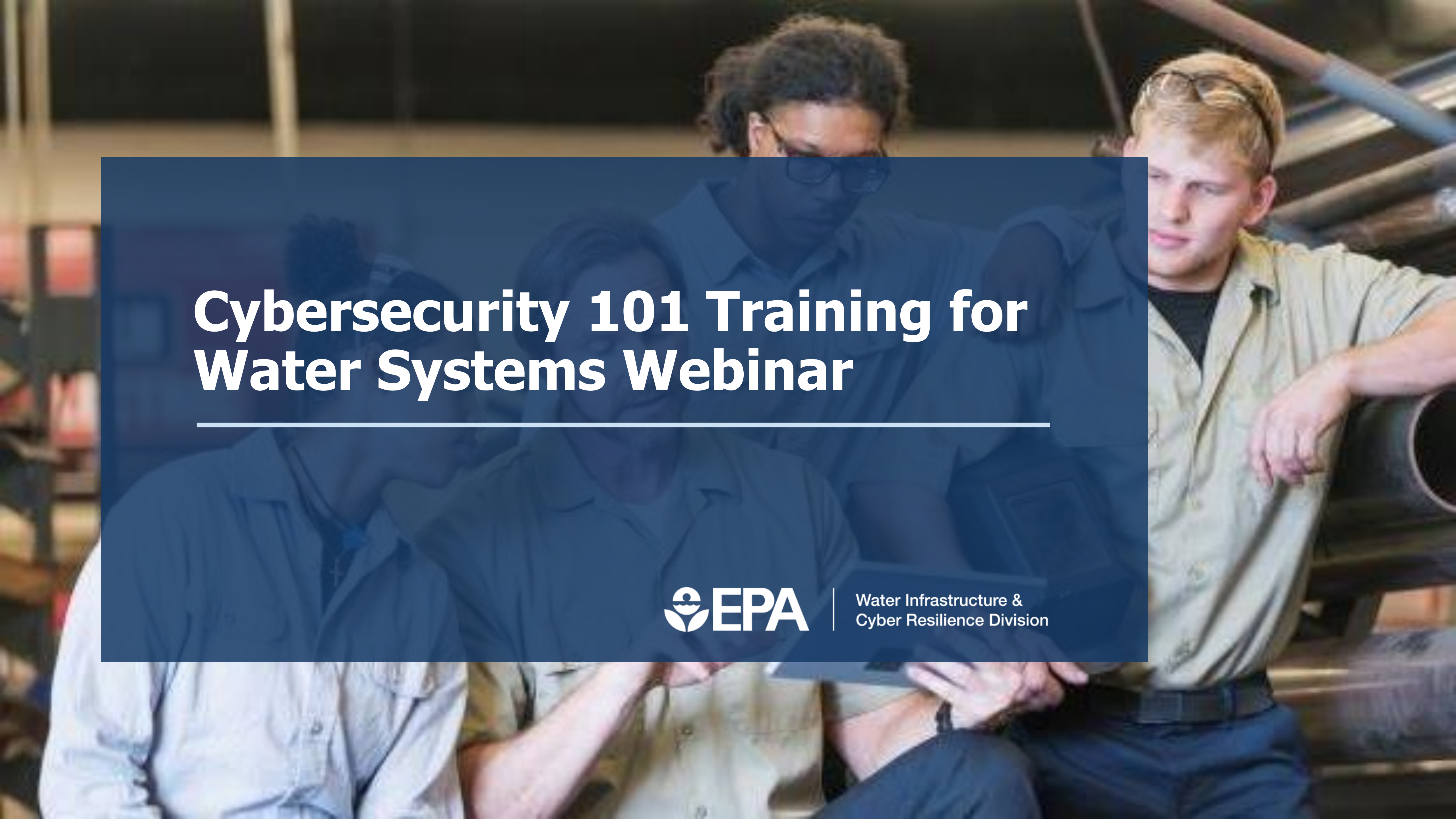


Cybersecurity 101 Training for Water Systems Webinar

EPA | Water Infrastructure & Cyber Resilience Division

Introduction

What is Cybersecurity?

Cybersecurity is the practice of ensuring confidentiality, integrity, and availability of information by protecting your digital systems and networks from unauthorized access or usage.

Why is Cybersecurity Important?

- Cybercrime cost victims a total of **$6.9 BILLION** in 2021
- Cybercrime is growing at about 15% each year
- Cybersecurity should be considered in all facets of life both personal and professional

Why is Cybersecurity Important for the Water Sector?

- **Cyber attacks could impact public health**
- **Cyber attacks could cause service disruptions**
- **Cyber criminals could gain access to protected employee and customer information**

Commonly Used Terms

Information Technology (IT)

The systems that collect, store, and process data.

Operational Technology (OT)

Hardware or software that detects or cause a change, through direct monitoring of industrial equipment.

Port

A virtual point where network connections start and end

Firewall

A device that restricts data communication traffic between two connected networks

Software

Programs and data stored in hardware and used by a computer

Hardware

The physical components of a system (computer, etc.)

Operating System

A software that controls the operation of a computer and directs the processing of programs

Cybersecurity 101 Overview for Water Systems

EPA | Water Infrastructure & Cyber Resilience Division

Key Steps to Establish and Manage a Cybersecurity Program

EPA | Water Infrastructure & Cyber Resilience Division

Step 1: Identify a Cybersecurity Lead

This individual should:

- Act as a centralized point of contact responsible for overseeing and managing the planning, resourcing, and execution of cyber activities for IT and OT systems.
- Be well-versed in different security technologies and understand how they work and be aware of the latest trends and information in IT and OT cybersecurity.

Step 2: Establish a Cybersecurity Policy

The primary purpose of cybersecurity policy is to enforce standards and procedures to protect your utility systems, prevent security breaches, and safeguard your networks.

Cybersecurity Policy typically includes:

- **Remote access policy** – offers guidelines for remote access to an organization’s network
- **Access control policy** – explains standards for network access, user access, and system software controls
- **Data protection policy** – provides guidelines for handling confidential data to avoid security breaches
- **Acceptable use policy** – sets standards for using the company’s IT and OT infrastructure

Step 3: Conduct Annual Cybersecurity Training

Cybersecurity awareness training highlights key concepts in an organization's IT/OT cybersecurity policy and outlines roles and responsibilities in cybersecurity.

This training should:

- Be tailored for ALL public water system personnel within your organization
- Focus on how to remain compliant with your organization’s cybersecurity policy
- Help to understand how to prevent cyber-attacks and protect system information
- Provide OT-specific cybersecurity training for those who use OT systems
- Be mandatory for all employees annually

Step 4: Prepare for Cybersecurity Threats

- Understand the current cyber **Tactics, Techniques, and Procedures (TTP)** to be better prepared and increase cyber resiliency.

- **TTPs** are the methods, tools, and strategies cyber threat actors use to develop and execute cyber-attacks.

- Sign up to receive CISA alerts and bulletins & stay aware of the latest TTPs
  - CISA Alerts provide timely information about current security issues, vulnerabilities, and exploits.
  - CISA Bulletins provide weekly summaries of new vulnerabilities, including Patch information when available.

Account Security

Never Use Default Passwords

A default password is a standard preconfigured password for a device or software. They are the default configuration for many devices and, if unchanged, present a serious security risk.

- ALWAYS change default passwords for all IT and OT systems
- In cases where default OT passwords can’t be changed, isolate the equipment and schedule to check logs for sign-ins

Password Security

Passwords provide the first line of defense against unauthorized access to an organization’s IT and OT systems and information.

- Enforce Password Length & Complexity- require all employees to create long and complex passwords that should at minimum be **eight characters** long and contain **one uppercase letter**, **one lowercase letter**, **one number**, **one symbol.**

- EXAMPLES: P@$$w0rD, iL^vE_C@t$, W@ter_$*CuR!ty

Require Separate IT and OT Credentials

Usernames and Passwords, also known as “credentials," should be different for users who access both IT and OT networks.

Username: ITUser2
Password: Pa$$w0rD

Username: OTUser2
Password: Il0v3w@t3r

Enable Multifactor Authentication (MFA)

MFA (also called “Two-Step Verification”) is a security feature that allows the user to present two pieces of evidence to confirm their identity:

- Something you know (password, PIN #, etc.)
- Something you have (smart card, smartphone)
- Something you are (fingerprint, facial recognition)

MFA is more secure because it eliminates the risk of hackers using stolen passwords and users reusing and sharing passwords.

Many IT and OT software platforms come with an option that will allow the IT/OT support staff to enable and configure MFA.

Manage User Privileges and Access

- Separate administrative accounts from common user accounts in order to ensure that common users and administrators **do not** have the same level of access.
  - Example: Creating other user accounts

- Disable or limit access to an account or network when access is no longer necessary.
  - Example: User relocated, terminated, etc.

Log Unsuccessful Login Attempts

Login block

- Login blocks lead to a locked account that can only be unlocked by resetting the password
- Too many unsuccessful login attempts by an account should trigger login block

Enable Email Security Controls

Security controls on emails can reduce common email-based threats such as:

- Spoofing
- Phishing
- Interception

Ensure all controls are enabled on corporate email structure

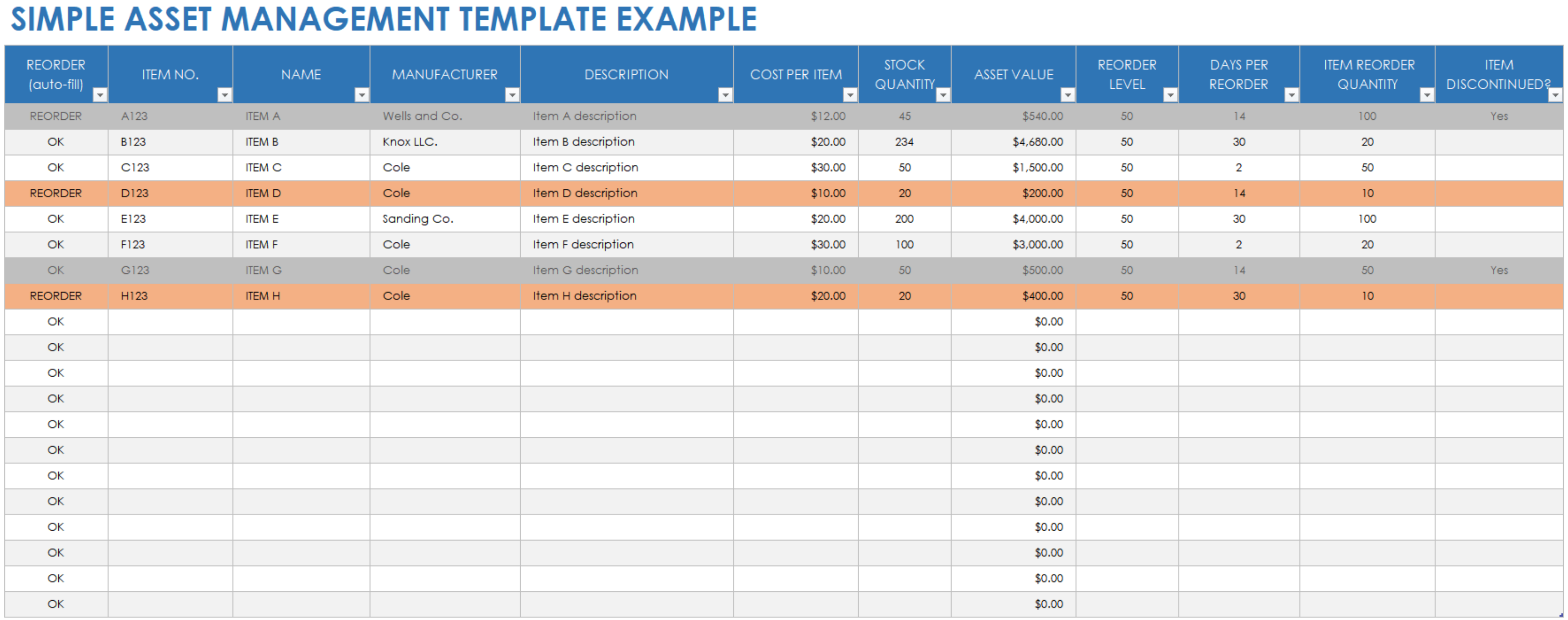
- Office 365 Outlook
- Google Workplace (Gmail)

Device Security

EPA | Water Infrastructure & Cyber Resilience Division

Maintain an Accurate Asset Inventory

An accurate inventory of IT and OT assets will help during the recovery phase of a cyber incident



SIMPLE ASSET MANAGEMENT TEMPLATE EXAMPLE

REORDER (auto-fill)	ITEM NO.	NAME	MANUFACTURER	DESCRIPTION	COST PER ITEM	STOCK QUANTITY	ASSET VALUE	REORDER LEVEL	DAYS PER REORDER	ITEM REORDER QUANTITY	ITEM DISCONTINUED?
REORDER	A123	ITEM A	Wells and Co.	Item A description	$12.00	45	$540.00	50	14	100	Yes
OK	B123	ITEM B	Knox LLC.	Item B description	$20.00	234	$4,680.00	50	30	20	
OK	C123	ITEM C	Cole	Item C description	$30.00	50	$1,500.00	50	2	50	
REORDER	D123	ITEM D	Cole	Item D description	$10.00	20	$200.00	50	14	10	
OK	E123	ITEM E	Sanding Co.	Item E description	$20.00	200	$4,000.00	50	30	100	
OK	F123	ITEM F	Cole	Item F description	$30.00	100	$3,000.00	50	2	20	
OK	G123	ITEM G	Cole	Item G description	$10.00	50	$500.00	50	14	50	Yes
REORDER	H123	ITEM H	Cole	Item H description	$20.00	20	$400.00	50	30	10	
OK							$0.00				
OK							$0.00				
OK							$0.00				
OK							$0.00				
OK							$0.00				
OK							$0.00				
OK							$0.00				
OK							$0.00				
OK							$0.00				
OK							$0.00				
OK							$0.00				
OK							$0.00				

Maintain Accurate Records of Software

Increase response and recovery times to a cyber incident as well as help with vulnerability management.

Maintain detailed records of critical IT and OT systems

- Firmware & Software versions
- Important configuration settings

Prohibit Unauthorized Hardware Connections

Unauthorized hardware should never be allowed to be connected to systems.

- USB thumb drives
- External hard drives
- Laptops
- Cell Phones

Be sure to emphasize this during your annual training!

Require Administrative Approval for New Software

Only network administrators should have the ability to install new software or firmware.

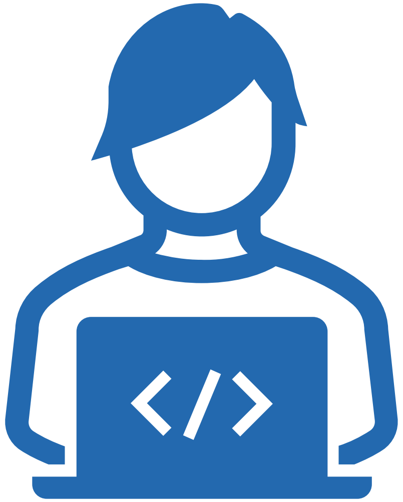
- This can be modified by enabling Admin Approval Mode in User Account Controls

Reduce the likelihood of a breach.

Disable Executable Code

Executable codes, such a Microsoft Office Macros, can be used by cyber criminals to discreetly install malware onto a computer or a network.

- Microsoft Office macros can be disabled within the Trust Center



Data Security

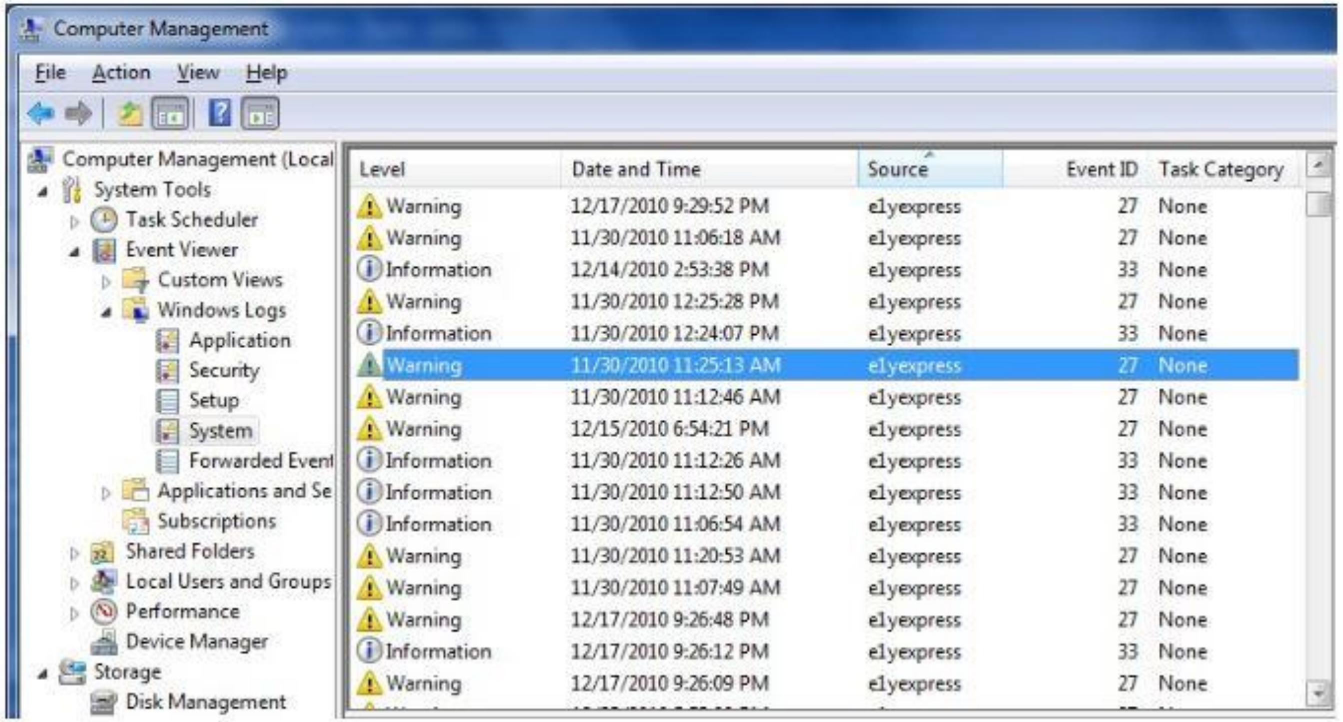
Collect Security Logs

Collecting security logs can help achieve better visibility to detect and effectively respond to a cyber incident.

Collect and store logs on network traffic related to security incidents and suspicious activity.

Protect Security Logs

Ensure logs are properly stored in a central system that can only be accessed by users who are both authorized and authenticated.



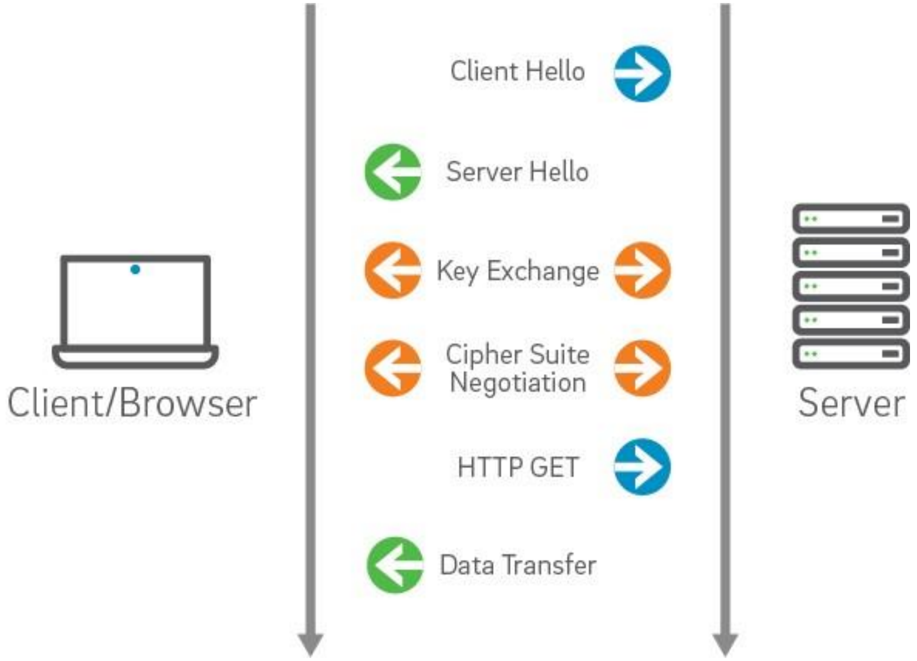
Level	Date and Time	Source	Event ID	Task Category
Warning	12/17/2010 9:29:52 PM	e1yexpress	27	None
Warning	11/30/2010 11:06:18 AM	e1yexpress	27	None
Information	12/14/2010 2:53:38 PM	e1yexpress	33	None
Warning	11/30/2010 12:25:28 PM	e1yexpress	27	None
Information	11/30/2010 12:24:07 PM	e1yexpress	33	None
Warning	11/30/2010 11:25:13 AM	e1yexpress	27	None
Warning	11/30/2010 11:12:46 AM	e1yexpress	27	None
Warning	12/15/2010 6:54:21 PM	e1yexpress	27	None
Information	11/30/2010 11:12:26 AM	e1yexpress	33	None
Information	11/30/2010 11:12:50 AM	e1yexpress	33	None
Information	11/30/2010 11:06:54 AM	e1yexpress	33	None
Warning	11/30/2010 11:20:53 AM	e1yexpress	27	None
Warning	11/30/2010 11:07:49 AM	e1yexpress	27	None
Warning	12/17/2010 9:26:48 PM	e1yexpress	27	None
Information	12/17/2010 9:26:12 PM	e1yexpress	33	None
Warning	12/17/2010 9:26:09 PM	e1yexpress	27	None

Use Effective Encryption

Enable Secure Socket Layer/Transport Layer Security (SSL/TLS)to protect data in transit

- Many web browsers have this enabled by default

https://www.epa.gov



Encrypt All Data

Data encryption can help maintain the confidentiality of sensitive data and integrity of both IT and OT networks.

- Do not store any sensitive data in a plain text format
- Only allow access to sensitive data to authorized and authenticated user

Vulnerability Management

EPA | Water Infrastructure & Cyber Resilience Division

Patch Known Vulnerabilities

- Patching systems and software can reduce the likelihood of cybercriminals exploiting known vulnerabilities to breach a network.
- Identify and install updates (patch) vulnerabilities as quickly as possible.
- If patching isn’t possible, perform enhanced monitoring.

Limit Internet Exposure

Limit internet exposure to systems and networks to close any potential weaknesses or vulnerabilities.

- Ensure systems do not have unnecessary internet exposure.
- Avoid connecting OT assets to the internet as much as possible.

Supply Chain/Third Party

Cyber Evaluation of IT and OT assets

When selecting IT and OT assets or services, ensure that cybersecurity is an important evaluation criterion.

Response and Recovery

Water Infrastructure &
Cyber Resilience Division

Create an Incident Response Plan

An incident response plan is a document with detailed procedures on how to respond to a cyber incident which can help minimize response and recovery times.

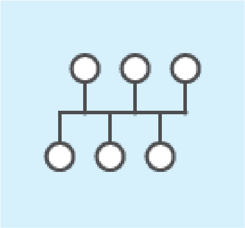
- Maintain and update ERP after incidents
- Conduct Tabletop Exercises (TTX) to improve incident response

Backup Systems Necessary for Operations

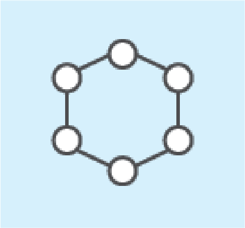
- Backup all systems that are necessary for operation.
- Reduce the likelihood and duration of data loss and loss of operation.
- Store backups separately from source system and test regularly.

Maintain Up-To-Date Network Documentation

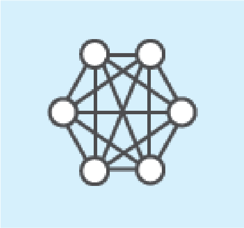
Reduce cyber-attack response times and maintain service continuity.



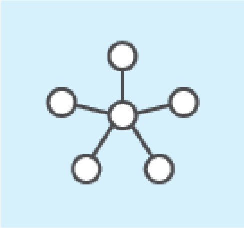
Bus
Directly connects devices to each other and transmits data between links.



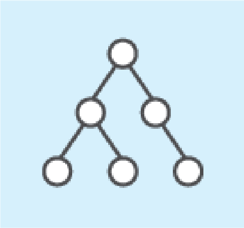
Ring
Connects devices next to each other in the form of a circle. Communication occurs unidirectionally or bidirectionally.



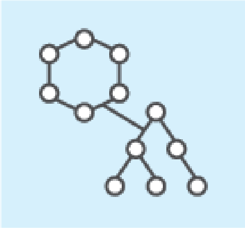
Mesh
Connects each device to every other device in the network.



Star
Features a central device which transmits data to other nodes in the system.



Tree
Connects devices down in a structure resembling a tree where parent nodes connect to child nodes.

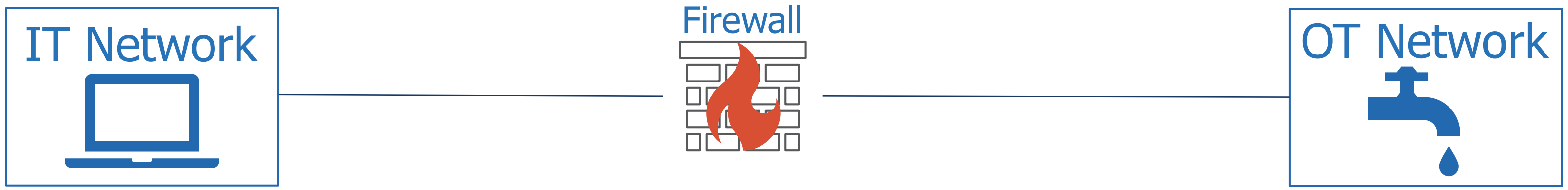


Hybrid
Consists of at least two different types of network topology.

Other Security Topics

Network Segmentation

Network segmentation is the separation of IT and OT networks by placing a barrier between them such as a firewall. It can help reduce the likelihood of the OT network being compromised if the IT network is compromised.



Adopt Cybersecurity Hygiene Principles

Cybersecurity hygiene refers to using the right technology, best practices, and user education to establish a healthy internal cybersecurity culture.

- Implementing the practices covered today, you can increase your ability to resist cyber threats and reduce the risk of a successful cyber-attack.

How to Report a Cyber Incident

Threat Response	Asset Response	EPA Response
Local Law Enforcement or	Cybersecurity & Infrastructure Security Agency (CISA) 888-282-0870 or report@cisa.gov	Environmental Protection Agency (EPA) Water Infrastructure and Cyber Resilience Division wicrd-outreach@epa.gov
FBI Field Office http://www.fbi.gov/contact-us/field		

Thank You

- Contact Us: WICRD-Outreach@EPA.gov

- Stay Up-To-Date:

www.epa.gov/waterriskassessment/epa-cybersecurity-best-practices-water-sector