gocyber COLLECTIVE

Introduction to Cybersecurity for Water and Wastewater Operators

Agenda

Day 1 (8:00 AM – 4:30 PM) - Understanding Cybersecurity Fundamentals and Industry Relevance

8:00 AM – 9:30 AM – Introduction to Cybersecurity

-Overview of cybersecurity: What is it and why it matters?

-Cyber threats: Understanding risks like malware, phishing, ransomware

-Basic cybersecurity terminology (e.g. firewall, encryption, VPN)

-Relevance to the water and wastewater sector

9:30 AM – 11:00 AM – Cyber Threats in the Water and Wastewater Industry

-Case studies of real-world incidents in the sector

-Common threat vectors: Social engineering, ransomware, insider threats

-Discussion: How cyber incidents could affect daily operations and safety

-Exercise: Identifying potential vulnerabilities in typical system components

11:00 AM – 11:15 AM – Break

11:15 AM – 12:45 PM – Cybersecurity Regulations and Standards for the Industry

-Overview of regulation (e.g. CISA guidelines, EPA standards

-Importance of compliance and reporting requirements

-Cybersecurity and physical security overlap

-Discussion: Consequences of non-compliance

12:45 PM – 2:45 PM – Basic IT and OT Concepts for Operators (Working Lunch)

-Difference between Information Technology (IT) and Operational Technology (OT)

-Common network components: SCADA systems, PLC's, HMI

-Basics of network architecture in water/wastewater systems

-Discussion: Understanding the network map of a typical facility

2:45 PM – 3:00 PM – Break

3:00 PM – 4:30 PM Introduction to Risk Management and Cyber Hygiene

-Identifying assets and assessing risks

-Simple steps for basic cyber hygiene: Strong passwords, regular updates

-The concept of the "human firewall" and social engineering awareness

-Exercise: Identifying good and bad practices in everyday operations

==

Day 2 - (8:00 AM – 3:30 PM) - Practical Cybersecurity Measures and Incident Response

8:00 AM – 9:30 AM – Securing the Water/Wastewater System

-Best practices for protecting SCADA and ICS

-Basic strategies for segmenting networks

-Physical security measures that support cybersecurity

-Discussion: Simple measures operators can take to enhance security

9:30 AM – 9:45 AM – Break

9:45 AM – 11:15 AM – Incident Response Basics

-What to do if a cyber incident occurs

-Steps for reporting incidents

-Introduction to incident response plans and procedures

-Exercise: Creating a basic incident response checklist

11:15 AM – 12:45 PM – Cybersecurity Tools for Non-IT Staff (Working Lunch)

-Overview of commonly used tools (antivirus software, firewalls, etc.)

-How to recognize signs of a compromised system

-Basic monitoring practices for operators

-Demonstration: What a suspicious email or system alert looks like

12:45 PM – 1:00 PM – Break

1:00 PM – 2:30 PM – Building a Cybersecurity Culture in the Workplace

-Importance of a security-focused culture

-Training and awareness programs for all staff levels

-Encouraging reporting of potential threats

-Discussion: How operators can advocate for cybersecurity in their roles

2:30 PM – 3:30 PM – Course Review and Q&A Session

-Recap of key concepts

-Open Q&A for further discussion and clarification

-Providing resources for further learning

-Feedback survey for CEU credit validation