CYBERSECURITY COURSE · SYLLABUS

Cybersecurity Training for Water and Wastewater Treatment Plants

Protect SCADA, PLCs and plant networks: CISA and EPA guidance, AWIA risk assessments, access control, segmentation, detection, incident response and recovery for water and wastewater utilities.

10	70	≈150	2,677	210	2,109
MODULES	LESSONS	EST. HOURS	SLIDES	SCENARIOS	FLASHCARDS

ABOUT THE COURSE

Cybersecurity Training for Water and Wastewater Treatment Plants is an online, self-paced course for operators, maintenance and I&C technicians, SCADA and IT staff, supervisors and managers at drinking-water and wastewater utilities. It is Virginia-oriented (SDWA §1433 with the Virginia Department of Health as primacy agency; Virginia Code § 2.2-5514 incident reporting for public bodies) and useful anywhere in the United States. Lessons cite public guidance from CISA, EPA, the FBI, NIST, AWWA and WaterISAC by name. The course is defensive only. Every lesson combines narrated slides with Key details, a pre-task checklist, field scenarios, worked examples, quizzes and flashcards.

Estimated study time: about 150 hours — roughly 15 hours per module, about 2 hours per lesson. **Prerequisites:** none; terms are explained for beginners. **Format:** online, any modern browser on phone, tablet or desktop; active study time is recorded.

What's included: 2,677 narrated slides, 70 labeled technical figures, 275 worked examples, 70 pre-task checklists, 210 field scenarios, 336 quiz questions, 2,109 flashcards, 11 narrated videos (a course introduction and one per module) and calculators & tools (Engineering calculator with 11 cybersecurity calculators).

COURSE SEQUENCE

CYB 101 Foundation · 75 hours · Modules 1–5

Cybersecurity Foundations: Threats, SCADA Architecture, CISA & EPA Frameworks, Governance & Access Control

- Explain why water and wastewater systems are targeted and how OT differs from IT, using real water-sector incidents.
- Describe SDWA §1433 (AWIA) cybersecurity duties, EPA enforcement findings, CIRCIA status and Virginia's 24-hour reporting rule.
- Map PLCs, RTUs, HMIs, historians, protocols, remote sites and vendor access onto the Purdue model and an industrial DMZ.
- Use NIST CSF 2.0, CISA CPGs 2.0, the AWWA assessment tool, ISA/IEC 62443 and the EPA checklist to assess a utility.
- Request and use CISA and EPA no-cost services: CSET, Cyber Hygiene scanning, architecture reviews and the Evaluation Program.
- Build a cyber risk register, policies, vendor requirements and a funded improvement plan with leadership accountability.
- Apply least privilege, strong passwords, phishing-resistant MFA, privileged-account control, secure remote access and physical protection.

CYB 102 Advanced · 75 hours · Modules 6–10

Network Defense, Detection, Incident Response, Recovery & Building a Utility Cyber Program

- Find and remove internet exposure, segment OT with firewalls, zones and conduits and secure radio and cellular telemetry.
- Harden PLCs, HMIs and servers, manage OT vulnerabilities with CISA KEV and advisories, and control removable media.
- Decide what to log, monitor OT networks and recognize abnormal HMI and process behavior as an operator.
- Run the first hour of a cyber incident: isolate, go to manual operation, protect public health and preserve evidence.
- Report incidents to CISA, the FBI, EPA, the state primacy agency and the Virginia Fusion Center within required times.
- Back up PLC logic and HMI projects (3-2-1, offline), set RTO/RPO and restore and validate OT after ransomware.
- Build a staged roadmap, write secure procurement specifications and measure program maturity over time.

COMPLETION & CERTIFICATES

A module certificate is issued when every lesson in the module is complete and the module quizzes average 80% or better. Each certificate lists active study hours and a verification code that can be checked on the Academy site.

REGULATIONS, EDITIONS & STANDARDS

SDWA §1433 (AWIA) · EPA water-sector cyber guidance · CISA CPGs 2.0 · NIST CSF 2.0 · NIST SP 800-82r3 · ISA/IEC 62443 · AWWA Cybersecurity Guidance

MODULES, LESSONS & OUTCOMES

1 Cybersecurity Foundations for Water & Wastewater Utilities

CYB 101 · 7 lessons · ≈15 hours

Water and wastewater plants now run on computers, and attackers know it. This module gives every operator, technician, supervisor and manager the foundation for the rest of the course. You will learn why utilities are targets, how plant control systems (OT) differ from office IT, who the threat actors are and what really happened in published water-sector incidents. We cover the federal rules under SDWA §1433 (AWIA), EPA enforcement and the pending CIRCIA reporting rule, the partners who help utilities for free, the cyber role every employee plays, and the daily hygiene habits that stop most attacks. Public health comes first: when the screen looks wrong, verify in the field.

LESSONS

1. Why water & wastewater systems are targets
2. IT vs OT: how plant control systems differ
3. Threat actors, motives & real water-sector incidents
4. Federal requirements: SDWA §1433 (AWIA), EPA enforcement & CIRCIA
5. Partners: CISA, EPA, FBI, WaterISAC & Virginia agencies
6. Roles & responsibilities: everyone defends the plant
7. Cyber hygiene basics for every employee

MODULE OUTCOMES — YOU WILL BE ABLE TO:

- Explain why drinking-water and wastewater utilities are attractive targets and what a cyber incident can do to public health, the environment and the utility.
- Describe the main ways attackers reach a utility, including internet-exposed PLCs and HMIs, remote access, phishing, vendors and removable media.
- Compare IT and OT priorities, lifecycles, patching limits and failure consequences, and explain why OT security puts safety and availability first.
- Identify the main threat actor types (nation-state, hacktivist, criminal, insider, accidental) and their typical motives and methods.
- Summarize published water-sector incidents and advisories from 2021 to 2026 using only what official sources confirm.
- State who SDWA §1433 (as amended by AWIA 2018) covers, what the risk and resilience assessment and emergency response plan must include, and the round-two deadlines.
- Describe EPA's May 2024 Enforcement Alert findings and the enforcement tools EPA can use, and explain the current status of CIRCIA reporting.
- Name the federal, sector and Virginia partners that help utilities (CISA, EPA, FBI, WaterISAC, Virginia Fusion Center, VDH ODW) and what each offers.
- Explain Virginia Code § 2.2-5514 reporting for public bodies and why reporting relationships should be built before an incident.
- Assign cyber responsibilities across leadership, the named cyber lead, operators, technicians, IT staff and vendors.
- Apply everyday cyber hygiene: strong passphrases, MFA, phishing awareness, removable-media rules, locked screens and fast reporting.
- Respond to suspicious HMI or process behavior by protecting public health first: notify the supervisor, verify with field instruments and lab samples, and go to manual control when directed.

2 SCADA & Control System Architecture

CYB 101 · 7 lessons · ≈15 hours

You cannot defend a plant control system you do not understand. This module walks through how SCADA really works at a water or wastewater utility: the PLCs, RTUs, HMIs, historians and engineering workstations that run the process; the industrial protocols they speak, such as Modbus, DNP3, EtherNet/IP and OPC UA; and how the Purdue model and an industrial DMZ organize the network into levels. You will trace telemetry to remote pump stations and

wells, map every remote access and vendor pathway, see why hardwired interlocks and practiced manual operation matter, and build an OT asset inventory and network drawings that make every later security step possible.

LESSONS

1. Control system components: PLCs, RTUs, HMIs, historians & engineering workstations
2. Industrial protocols: Modbus, DNP3, EtherNet/IP & OPC UA
3. The Purdue model, network levels & the industrial DMZ
4. Remote sites: pump stations, telemetry, radio & cellular links
5. Remote access & vendor connection pathways
6. Safety systems, hardwired interlocks & manual fallback
7. OT asset inventory & network documentation

MODULE OUTCOMES — YOU WILL BE ABLE TO:

- Identify the main components of a water or wastewater control system and describe what each one does.
- Explain how PLCs and RTUs read field instruments, run logic and drive pumps, valves and chemical feeders.
- Describe why engineering workstations, project files and PLC run/program modes deserve special protection.
- Compare Modbus, DNP3, EtherNet/IP and OPC UA, including which have built-in security and which do not.
- Scale raw register and 4-20 mA values to engineering units to sanity-check what the HMI displays.
- Place plant assets on the Purdue model levels and explain the job of the industrial DMZ.
- Trace the telemetry path from a remote pump station or well to the central SCADA system and name its weak points.
- Map every remote access and vendor connection pathway, sanctioned and unsanctioned, and rank them by risk.
- Explain how hardwired interlocks, mechanical limits and independent safety systems protect public health when software fails or is manipulated.
- Plan and practice manual operation so the plant can run safely if SCADA is lost or untrusted.
- Build and maintain an OT asset inventory using the five steps in CISA's 2025 asset inventory guidance.
- Keep network drawings, data-flow diagrams and change records accurate enough to support response and recovery.

3 Frameworks, Standards & Cyber Assessments

CYB 101 · 7 lessons · ≈15 hours

Cybersecurity guidance for water utilities can feel like alphabet soup: CSF, CPG, WCAT, CSET, 62443, 800-82, AWIA. This module sorts it out for plant people. You will learn how NIST CSF 2.0 gives a common structure with six functions, how CISA's Cybersecurity Performance Goals (CPG 2.0) set a short list of high-impact practices, and how the AWWA guidance and assessment tool turn your technology use into a prioritized control list. You will see what ISA/IEC 62443 and NIST SP 800-82 Rev. 3 add for control systems, which free EPA and CISA assessments and services exist, and how cybersecurity must appear in your SDWA §1433 (AWIA) risk and resilience assessment and emergency response plan.

LESSONS

1. NIST Cybersecurity Framework 2.0
2. CISA Cybersecurity Performance Goals
3. AWWA Cybersecurity Guidance & Assessment Tool
4. ISA/IEC 62443 & NIST SP 800-82 for OT
5. EPA cybersecurity checklist & the Water Sector Cybersecurity Evaluation Program
6. CISA no-cost services: CSET, scanning, architecture reviews & advisors
7. Cybersecurity in the AWIA risk & resilience assessment

MODULE OUTCOMES — YOU WILL BE ABLE TO:

- Describe the six NIST CSF 2.0 functions and give a plant example for each.
- Build a simple CSF Current Profile and Target Profile and identify the gaps.
- Explain the purpose of CISA's Cross-Sector Cybersecurity Performance Goals (CPG 2.0) and how they map to the CSF.
- Choose an AWWA assessment path (Small System, AWWA Assessment or CSET import) for a given utility.
- Explain ISA/IEC 62443 zones, conduits, security levels and the asset owner, integrator and supplier roles.
- Use NIST SP 800-82 Rev. 3 as a reference for applying security controls to OT without harming operations.
- Compare EPA's Water Cybersecurity Assessment Tool, the Water Sector Cybersecurity Evaluation Program and the EPA

Cybersecurity Technical Assistance Program.
- Identify CISA's no-cost services, including Cyber Hygiene vulnerability scanning, CSET, VADR and Cybersecurity Advisors, and how to request them.
- State which community water systems must certify a risk and resilience assessment and ERP under SDWA §1433 and the current recertification dates.
- Include 'electronic, computer, or other automated systems' in an RRA using threat, vulnerability and consequence estimates.
- Turn assessment findings into a prioritized, funded risk mitigation plan with owners and dates.
- Apply the rule that no assessment, scan or test touches production OT without written authorization, operations approval and a manual-operation plan.

4 Cyber Governance, Risk Management & Policy

CYB 101 · 7 lessons · ≈15 hours

Cybersecurity at a water or wastewater utility fails most often for reasons that are not technical: nobody owns it, risks are never written down, policies sit in a binder, vendors connect however they like, and leaders never see a clear picture. This module builds the management system that keeps plant-floor security working. You will set up governance with a named cyber lead and clear accountability, score risks by likelihood and consequence in a risk register, write the policies a utility actually needs, manage vendor and supply-chain risk, build a phased budget using SRF and grant options, run role-based training, and report simple metrics that drive continual improvement.

LESSONS

1. Governance: leadership, a named cyber lead & accountability
2. Cyber risk assessment: likelihood, consequence & the risk register
3. Policies, standards & procedures a utility needs
4. Vendor, integrator & supply-chain risk
5. Budgeting & funding cybersecurity: SRF, grants & phased plans
6. Workforce training & security awareness programs
7. Metrics, reporting to leadership & continual improvement

MODULE OUTCOMES — YOU WILL BE ABLE TO:

- Explain why cybersecurity governance is a leadership duty and how the NIST CSF 2.0 Govern function and CISA CPG 2.0 frame it.
- Define the role, authority and reporting line of a named cybersecurity lead, including OT responsibilities shared with operations.
- Build a simple RACI that assigns cyber tasks across leadership, IT, operations, maintenance, vendors and the cyber lead.
- Score cyber risks with likelihood and consequence scales and place them on a risk matrix that puts public health first.
- Maintain a risk register with owners, treatment decisions, due dates and documented risk acceptance.
- Calculate single loss expectancy, annualized loss expectancy and residual risk to compare control options.
- Distinguish policies, standards, procedures and guidelines and list the core cyber policies a utility needs.
- Assess, contract, onboard, monitor and offboard vendors and integrators using EPA and CISA procurement guidance.
- Build a phased cybersecurity budget that starts with no-cost actions and uses SRF, grant and capital funding where eligible.
- Design role-based awareness training for operators, technicians, office staff and leaders, and measure its effect.
- Select and calculate metrics such as MFA coverage, patch age against target and MTTD/MTTR, and report them to leadership.
- Run a plan-do-check-act cycle that turns assessments, incidents and exercises into tracked corrective actions.

5 Identity, Access & Physical Security

CYB 101 · 7 lessons · ≈15 hours

Most water-sector cyber incidents start with an account, not exotic malware: a default password left on an internet-facing PLC, one login shared by every operator, a former employee who can still sign in, or a vendor remote-access tool that is always on. EPA's May 2024 Enforcement Alert found exactly these gaps at many inspected systems. This module teaches plant staff how to control who can do what on SCADA, HMIs, PLCs and business systems: roles and least privilege, strong passwords and passphrases, multifactor authentication including phishing-resistant MFA, privileged and shared accounts, joiner-mover-leaver processes, secure remote access through jump hosts, and the physical security that keeps people away from panels, cabinets and control rooms they should not touch.

LESSONS

1. Accounts, roles & least privilege
2. Passwords, default credentials & passphrases
3. Multifactor authentication, including phishing-resistant MFA
4. Privileged & shared accounts in control systems
5. Onboarding, role changes & offboarding (joiners, movers, leavers)
6. Secure remote access: VPNs, jump hosts & session control
7. Physical security that protects cyber assets

MODULE OUTCOMES — YOU WILL BE ABLE TO:

- Explain least privilege and role-based access and apply them to operator, supervisor, technician, engineer, IT and vendor roles.
- Build a simple access matrix that maps plant roles to HMI, SCADA, PLC and business-system permissions.
- Identify default, weak and shared credentials and describe why EPA and CISA rank changing them as a top action.
- Calculate password and passphrase strength in bits and compare length with complexity.
- Describe the factors of authentication and rank common MFA methods from weakest to phishing-resistant.
- Decide where MFA is required first (remote access, email, administrator and cloud accounts) and where compensating controls fit at plant consoles.
- Separate privileged from everyday accounts and describe how a password vault, check-out and rotation reduce risk.
- Replace or control shared operator logins without slowing response at the HMI.
- Run a joiner-mover-leaver process that grants, changes and removes access, keys and badges on time.
- Describe a secure remote-access path using MFA, a jump host, approval, time limits and session logging.
- Apply layered physical security to control rooms, PLC panels and remote sites such as lift stations and wells.
- Recognize which access changes to a production control system require written authorization, operations approval and a rollback plan.

6 Network Defense & OT Hardening

CYB 102 · 7 lessons · ≈15 hours

Many 2024-2026 attacks on water and wastewater control systems needed no clever malware. They reached a PLC, HMI or cellular modem that was directly on the internet, often with a default or weak password. This module shows plant staff how their control network works and how to defend it. You will learn IP addresses, ports, switches and routers in plain terms; how to find and remove internet exposure with free CISA services and your own records; how segmentation, firewalls, zones and conduits contain trouble; how to secure radio and cellular telemetry; how to harden PLCs, HMIs and servers; how to run risk-based patching with the KEV catalog; and how allowlisting and removable-media controls protect endpoints.

LESSONS

1. Network basics for plant staff: IP addresses, ports, switches & routers
2. Finding and removing internet exposure
3. Segmentation, firewalls, zones & conduits
4. Wireless, radio & cellular telemetry security

MODULE OUTCOMES — YOU WILL BE ABLE TO:

- Explain IP addresses, subnets, gateways, ports, switches, routers and firewalls using plant examples.
- Calculate usable host counts for common subnet sizes and read a simple plant network drawing.

5. Secure configuration & hardening of PLCs, HMIs and servers
6. Vulnerability & patch management in OT
7. Endpoint protection, allowlisting & removable media

- Identify the common ways control systems become reachable from the internet, including port forwarding, cellular modems and vendor remote tools.
- Describe how to confirm and remove internet exposure using the asset inventory, firewall reviews and CISA Cyber Hygiene scanning of the utility's own addresses.
- Apply the Purdue model and ISA/IEC 62443 zones and conduits to separate IT, the industrial DMZ and control networks.
- Write or review firewall rules that follow default-deny, least-privilege and documented-business-need principles.
- Explain the security weaknesses of licensed radio, spread-spectrum radio, Wi-Fi and cellular telemetry and the controls that reduce them.
- Build a hardening baseline for PLCs, HMIs, engineering workstations and servers, including default passwords, unused services and the PLC key switch.
- Prioritize OT vulnerabilities using the CISA KEV catalog, CVSS v4.0, exposure and process consequence.
- Plan an OT patch through testing, an approved maintenance window, rollback and verification, and record compensating controls when patching must wait.
- Describe application allowlisting, endpoint protection and removable-media controls suited to control-system computers.
- State the authorization, operations-approval, vendor-coordination and manual-operation steps required before any change to a production control system.

7 Monitoring, Detection & Threat Awareness

CYB 102 · 7 lessons · ≈15 hours

Most water-sector cyber incidents are found late, by an operator who notices something odd or a vendor who calls with bad news. This module teaches how a utility sees trouble early. You will learn which IT and OT logs to collect and keep, how passive network monitoring and OT-aware intrusion detection watch plant protocols without touching the process, and how operators act as sensors for abnormal HMI and process behavior. It covers phishing, social engineering and ransomware warning signs, using CISA, EPA, FBI and WaterISAC threat intelligence and MITRE ATT&CK for ICS, checking process integrity with lab and field measurements, and practical monitoring options for small utilities.

LESSONS

1. Logging: what to collect in IT and OT
2. Network monitoring & OT intrusion detection
3. The operator as a sensor: spotting abnormal HMI and process behavior
4. Phishing, social engineering & ransomware warning signs
5. Threat intelligence: advisories, WaterISAC & MITRE ATT&CK for ICS
6. Verifying process integrity: lab, field & independent checks
7. Security monitoring options for small utilities

MODULE OUTCOMES — YOU WILL BE ABLE TO:

- List the IT and OT log sources a water or wastewater utility should collect, and explain why accurate time stamps and protected storage matter.
- Estimate log storage needs from event rate, event size and retention period.
- Explain how passive network monitoring with SPAN ports or network TAPs and OT-aware intrusion detection work without sending traffic to controllers.
- Describe a network baseline and the OT alerts that matter most, such as new devices, new connections, PLC program downloads and mode changes.
- Recognize abnormal HMI and process behavior that may signal a cyber event and respond by verifying, reporting and protecting the process.
- Perform a chemical-feed sanity check to decide whether an HMI setpoint or reading is physically reasonable.

- Identify the warning signs of phishing, business email compromise, phone pretexting, MFA push fatigue and pre-ransomware activity.
- Use joint CISA, FBI, EPA and NSA advisories, the KEV catalog, WaterISAC and the Virginia Fusion Center to turn threat information into plant actions.
- Map observed adversary behavior to MITRE ATT&CK for ICS tactics such as Inhibit Response Function and Impair Process Control.
- Verify process integrity with independent checks: lab samples, local gauges, hardwired instruments, chemical drawdown and mass balance.
- Compare monitoring options for small utilities, including in-house review, managed security service providers, free CISA scanning and sector programs.
- Calculate and use detection metrics such as mean time to detect (MTTD), mean time to respond (MTTR), log coverage and alert volume.

8 Cyber Incident Response & Reporting

CYB 102 · 7 lessons · ≈15 hours

A cyber incident at a water or wastewater utility is first a public-health and environmental event, then an IT problem. This module teaches plant staff how to respond when something looks wrong on the HMI or the business network. You will build and staff a written cyber incident response plan tied to the AWIA emergency response plan, take safe first actions, run the plant in manual with field and lab checks, and report on time to CISA, the FBI, EPA, your state primacy agency and, for Virginia public bodies, the Virginia Fusion Center within 24 hours. You will also learn to preserve evidence, communicate with staff, customers and media, and improve through tabletop exercises and after-action reviews.

LESSONS

1. The cyber incident response plan & team
2. First actions when a cyberattack is suspected
3. Manual operation & keeping water safe during an incident
4. Reporting: CISA, FBI, EPA, state primacy & the Virginia Fusion Center
5. Evidence preservation & working with investigators
6. Communications: staff, customers, media & public notification
7. Tabletop exercises & after-action improvement

MODULE OUTCOMES — YOU WILL BE ABLE TO:

- Describe the parts of a cyber incident response plan and how it links to the SDWA §1433 emergency response plan.
- Assign incident response roles, including an incident commander, OT lead, IT lead, communications lead and an after-hours call tree.
- Recognize the signs that an HMI, PLC or business-system problem may be a cyber incident and escalate it without delay.
- Take safe first actions: protect the process, go to manual when integrity is in doubt, contain without wiping, and write down what you see.
- Operate key treatment and collection processes manually and verify water quality with field instruments and lab samples.
- Identify the correct reporting channels (CISA, FBI/IC3, EPA, the state primacy agency, the Virginia Fusion Center and WaterISAC) and what each needs.
- Apply Va. Code § 2.2-5514(C) to report incidents at public bodies to the Virginia Fusion Center within 24 hours of discovery.
- Explain the status of CIRCIA reporting and the need to verify current federal rules before relying on them.
- Preserve volatile and physical evidence with a chain of custody and support law enforcement and investigators.
- Plan clear, accurate communications to staff, leadership, customers, media and regulators, including public notification when water quality is affected.
- Plan, run and evaluate a cyber tabletop exercise and turn after-action findings into a tracked improvement plan.

- Calculate reporting deadlines, response-time metrics, chemical-dose checks and storage time to support incident decisions.

9 Backup, Recovery & Cyber Resilience

CYB 102 · 7 lessons · ≈15 hours

Every utility will eventually lose a server, a PLC program or a whole network to ransomware, a bad update or a failed disk. What matters is how fast you can get back to safe, normal operation. This module shows how to build a 3-2-1 backup strategy with offline and immutable copies, and how to capture PLC logic, HMI projects, firmware and network device configurations. You will run a business impact analysis, set RTO and RPO targets and check them with simple math. The module then works through ransomware recovery decisions, validating OT systems before return to service, cyber content in the AWIA emergency response plan and continuity of operations, and cyber insurance, legal and contract issues.

LESSONS

1. Backup strategy: 3-2-1, offline & immutable copies
2. Backing up PLC logic, HMI projects & device configurations
3. Business impact analysis, RTO & RPO
4. Ransomware recovery: decisions & sequence
5. Restoring and validating OT systems before return to service
6. Cyber in the emergency response plan & continuity of operations
7. Cyber insurance, legal & contract considerations

MODULE OUTCOMES — YOU WILL BE ABLE TO:

- Explain the 3-2-1 backup rule and why at least one copy must be offline or immutable.
- Compare full, incremental and differential backups, snapshots and image backups for IT and OT systems.
- Build an OT backup list that covers PLC and RTU logic, HMI and SCADA projects, historians, firmware and network device configurations.
- Verify a backup with a hash, a program compare and a documented restore test.
- Conduct a simple business impact analysis that ranks essential plant functions by public-health consequence.
- Set and check recovery time objectives (RTO) and recovery point objectives (RPO) against backup schedules and restore times.
- Calculate backup size, transfer time, storage needed for a retention policy and availability or downtime percentages.
- Describe the main decisions and the safe sequence for recovering IT and OT systems after ransomware.
- Validate a restored control system with logic compares, I/O and loop checks, alarm tests and lab verification before return to service.
- Describe the cyber content an AWIA emergency response plan and a continuity of operations plan should contain, including manual operation.
- Explain what cyber insurance typically covers and excludes and what the utility must do to keep coverage.
- Identify backup, recovery, notification and security clauses to include in vendor, integrator and cloud contracts.

10 Building & Sustaining a Utility Cybersecurity Program

CYB 102 · 7 lessons · ≈15 hours

Cybersecurity is not a one-time project; it is a program a utility runs every year, like lab QA or asset management. This capstone module shows small and medium water and wastewater utilities how to turn the practices from Modules 1 to 9 into a phased, funded roadmap. You will learn to build security into new projects and procurement specifications, including SRF-funded work, and to manage cloud, IoT, AMI and smart-water systems. The lessons cover today's threats, from nation-state prepositioning to the 2026 PLC campaigns, how to measure maturity and close findings, how to work with IT, integrators and neighboring utilities, and how to keep learning through free CISA, EPA and WaterISAC resources.

LESSONS

1. A practical roadmap for small and medium utilities

MODULE OUTCOMES — YOU WILL BE ABLE TO:

2. Secure-by-design projects, procurement specifications & SRF-funded work
3. Cloud, IoT, AMI & smart-water technologies
4. Emerging threats: nation-state prepositioning, AI & PLC campaigns
5. Measuring maturity: self-assessments, audits & corrective actions
6. Working with IT, integrators, contractors & neighboring utilities
7. Cyber careers, professional development & course wrap-up

- Build a phased 30-, 90- and 365-day cybersecurity roadmap for a small or medium utility using the EPA/CISA/FBI Top Cyber Actions and the 2025 Primary Mitigations for OT.
- Rank roadmap actions by risk reduction, cost and effort, starting with internet exposure, default passwords and remote access.
- Write cybersecurity requirements into design, bid and integration contracts using CISA Secure by Demand and the EPA Cybersecurity Procurement Checklist.
- Explain how SRF and other funding programs can pay for cybersecurity components of projects, and where to verify current eligibility.
- Describe the security risks and shared responsibilities of cloud SCADA, hosted historians, cellular modems, IoT sensors and AMI.
- Summarize the 2023 to 2026 threats to water systems, including Volt Typhoon prepositioning, CyberAv3ngers, pro-Russia hacktivists and the 2026 PLC campaigns.
- Explain how AI changes phishing and social engineering, and set simple rules for using AI tools with utility data.
- Choose an appropriate self-assessment or third-party assessment and compare current and target maturity.
- Turn assessment findings into a corrective action plan with owners, dates, verification and leadership reporting.
- Define who does what among utility operations, IT, integrators, vendors, managed service providers and mutual-aid partners.
- Use information-sharing communities and free services from CISA, EPA, WaterISAC, AWWA and Virginia agencies to sustain the program.
- Plan your own next steps in OT cybersecurity learning and identify careers that blend plant operations with cybersecurity.

STUDY-HOUR PLAN

Module	Course	Lessons	Est. hours
1. Cybersecurity Foundations for Water & Wastewater Utilities	CYB 101	7	≈15
2. SCADA & Control System Architecture	CYB 101	7	≈15
3. Frameworks, Standards & Cyber Assessments	CYB 101	7	≈15
4. Cyber Governance, Risk Management & Policy	CYB 101	7	≈15
5. Identity, Access & Physical Security	CYB 101	7	≈15
6. Network Defense & OT Hardening	CYB 102	7	≈15
7. Monitoring, Detection & Threat Awareness	CYB 102	7	≈15
8. Cyber Incident Response & Reporting	CYB 102	7	≈15
9. Backup, Recovery & Cyber Resilience	CYB 102	7	≈15
10. Building & Sustaining a Utility Cybersecurity Program	CYB 102	7	≈15
Total		**70**	**≈150**

IMPORTANT NOTICE

Prepared with AI assistance. Training only — verify against current CISA, EPA and FBI guidance, your state primacy agency, your utility's written cybersecurity, incident response and emergency response plans, and vendor instructions.

Always verify against the current CISA, EPA, FBI and NIST publications cited in each lesson, Safe Drinking Water Act §1433 (America's Water Infrastructure Act) requirements, Virginia Code § 2.2-5514 and your state primacy agency, your utility's written cybersecurity policies, incident response and emergency response plans, and your control-system vendors' instructions. This course does not replace a professional cybersecurity assessment, your IT/OT security staff, legal counsel or law enforcement. Never test, scan or change a production control system without written authorization, operations approval and a rollback plan; never access systems you are not authorized to use.

Certificates record completion; CEU/CPE credit is subject to approval by your licensing board or employer. Independent training, not affiliated with or endorsed by any licensing board or standards body. The course is not endorsed by CISA, EPA, the FBI or any other agency, does not satisfy SDWA §1433 requirements on its own and does not replace a cybersecurity assessment or the training, authorization and access controls your utility must provide.

© 2026 TRYeTECH · TRY Enviro Technologies LLC · support@tryetech.com · Start free at tryetech.com/academy — Module 1, Lesson 1 opens without an account.