Anonymous Cybersecurity Survey for U.S. Water and Wastewater Utilities

Welcome to the Survey

Terms Used in the Survey

- DCS - Distributed Control System. A type of control system.
- DMZ - Demilitarized Zone. A network area between IT and OT system that can provide extra security
- HMI - Human Machine Interface. A computer display that lets an operator see and interact with the operations process.
- ICS - Industrial Control System. A more generic term for DCS or SCADA systems.
- IT - Information Technology. Computer hardware and software and communication equipment used to run the enterprise/business.
- MFA - Multi-Factor Authentication. Using more than one means to authenticate a user.
- OT - Operational Technology. Computer hardware and software and communication equipment used to run the water or wastewater process.
- PLC - Programmable Logic Controller. An industrial computer that runs a process
- SCADA - Supervisory Control and Data Acquisition. A type of control system.

WATER ISAC

Anonymous Cybersecurity Survey for U.S. Water and Wastewater Utilities

Respondent and Organization

1. Primary role(s) of the respondent(s). Select all that apply:

- [ ] CISO or Sr. Security Analyst
- [ ] CIO or IT manager or IT specialist
- [ ] Operations Director or Engineer
- [ ] Superintendent or Operator
- [ ] Executive management or Board member
- [ ] Consultant or managed security service provider
- [ ] Legal staff
- [ ] Other (please specify)

2. What services does your utility provide? Select all that apply:

- [ ] Drinking Water
- [ ] Wastewater
- [ ] Raw water
- [ ] Storm water
- [ ] Dam operations

3. How many individuals (not accounts) does your system serve?

- ◯ <= 500
- ◯ 501 - 3,300
- ◯ 3,301 - 10,000
- ◯ 10,001 - 50,000
- ◯ 50,001 - 100,000
- ◯ 100,001 - 250,000
- ◯ > 250,000

4. What is your utility's total staff count?

- ◯ < 5
- ◯ 5 - 20
- ◯ 21 - 50
- ◯ 51 - 150
- ◯ 151 - 300
- ◯ 301 - 600
- ◯ > 600

5. Describe your operational control system:

- ◯ Completely manual with local alarms
- ◯ Completely manual with local and remote alarms
- ◯ Manual control with some local automation and remote alarms
- ◯ Packaged skid or local system automation with remote alarms
- ◯ Integrated SCADA or DCS system with intermittent Operations Control Center coverage and remote coverage when not staffed
- ◯ Integrated SCADA or DCS System with 24/7/365 Operations Control Center coverage
- ◯ Not sure
- ◯ Other (please specify)

6. Can you operate your system manually (in hand or local) without networked PLCs, the SCADA system or DCS system available? Select all that apply.

- ☐ Yes, whole system
- ☐ Yes, Distribution system
- ☐ Yes, Collection system
- ☐ Yes, Wastewater treatment system
- ☐ Yes, Water treatment system
- ☐ Yes, some components of the system
- ☐ No, but we are working on being able to
- ☐ No
- ☐ Not sure
- ☐ Other (please specify)

7. Describe your approach for remote connections to the control system. Select all that apply.

- [ ] Not applicable, we do not have any remote external connections (internet connection, etc.) to the control system
- [ ] Alarm call-outs
- [ ] Dial in modem
- [ ] Software such as VNC, RealVNC, Team Viewer, RemotePC, Logmein, etc.
- [ ] Remote Desktop Procedure (RDP)
- [ ] Virtual Private Network (VPN)
- [ ] Combined with multi-factor authentication (MFA)
- [ ] Jump box in the control network
- [ ] Jump box in a control network DMZ
- [ ] Temporary remote connection authorized by and activated by Operations Control Center staff
- [ ] Other (please specify)

8. Describe the type of equipment used by staff for remote system monitoring or control. Select all that apply.

- [ ] On premise utility-owned desktop computer
- [ ] Off premise utility-owned desktop, laptop, tablet or cell phone
- [ ] Off premise employee-owned desktop, laptop, tablet or cell phone
- [ ] Combined with management software that checks the remote device for security compliance before making the connection
- [ ] Not sure
- [ ] Other (please specify)

Anonymous Cybersecurity Survey for U.S. Water and Wastewater Utilities

Security Program

9. Is there one manager at your utility who is assigned to and widely recognized as being responsible for all cybersecurity?

- ◯ Yes, one person is responsible for both IT and OT cybersecurity
- ◯ Yes, one person is responsible for IT cybersecurity, our OT system does not use computers or PLCs
- ◯ No, different people are responsible for IT and OT cybersecurity
- ◯ No, there is only someone responsible for OT, we do not have anyone responsible for IT cybersecurity
- ◯ No, a committee or group oversees cybersecurity
- ◯ No
- ◯ Not sure
- ◯ Other (please specify)

10. How many full-time equivalent people (FTEs) work on IT cybersecurity for your utility, including contractors and municipal or county staff?

- ◯ 0
- ◯ 0.5
- ◯ 1
- ◯ 2
- ◯ 3-5
- ◯ > 5
- ◯ Not sure

11. How many full-time equivalent people (FTEs) work on OT cybersecurity for your utility, including contractors and municipal or county staff?

- ◯ 0
- ◯ 0.5
- ◯ 1
- ◯ 2
- ◯ 3-5
- ◯ > 5
- ◯ Not sure

12. What cybersecurity threats are your utility most concerned about? Select all that apply.

- ☐ Ransomware
- ☐ Business email compromise / vendor email compromise
- ☐ Targeted attack by a state actor (Russia, China, North Korea, Iran, etc.)
- ☐ Collateral damage from a state actor (WannaCry, NotPeta, etc.)
- ☐ Insider threat
- ☐ Something against the IT / enterprise network
- ☐ Something against the OT / ICS / control system network
- ☐ All of the above
- ☐ We are pretty small so threats are not too likely
- ☐ None
- ☐ Other (please specify)

WATER ISAC

Anonymous Cybersecurity Survey for U.S. Water and Wastewater Utilities

Risk Management

13. Do you have written security policies and procedures that you follow and enforce?

- ◯ No, not yet
- ◯ Currently working on it
- ◯ Yes, for IT
- ◯ Yes, for OT
- ◯ Yes, for both IT and OT
- ◯ Not sure
- ◯ Other (please specify)

14. Do you have a written cybersecurity incident response plan? Select all that apply.

- ☐ Not yet
- ☐ Currently working on it
- ☐ Yes, a basic one with internal and external contact information
- ☐ Yes, a more comprehensive one that includes contact information, isolation steps, response steps and recovery steps
- ☐ We hold at least one tabletop cybersecurity incident response exercise each year
- ☐ We practice manual operations of our water or wastewater system at least once a year in case the SCADA or DCS system become unavailable
- ☐ Not sure
- ☐ Other (please specify)

15. What is the degree of segmentation/separation between OT and IT systems? Select all that apply.

- [ ] No formal separation (flat network)
- [ ] Virtual local area networks (VLAN)
- [ ] Router separating networks
- [ ] Firewall separating networks
- [ ] Firewall with demilitarized zone (DMZ)
- [ ] Back-to-back firewalls from different vendors
- [ ] Deep-inspection firewall
- [ ] Data diode
- [ ] No network connection between the two systems
- [ ] We also segment within the OT network by placing a firewall between the HMI’s (level 2) and the controllers or PLCs (level 1)
- [ ] Not sure
- [ ] Other (please specify)

16. Are you using an advanced cybersecurity monitoring solution to detect intrusions? This would be something more involved than just an antivirus or anti-malware solution and might include features like: continuous asset detection, traffic-flow anomaly detection, baseline changes, file changes, indicator of compromise (IOC) detection, tactics, techniques and procedure (TTP) detection, and traffic logging. Select all that apply.

- [ ] Yes, on the IT side
- [ ] In the planning stage on the IT side
- [ ] Considering it on the IT side
- [ ] Yes, on the OT / ICS side
- [ ] In the planning stage on the OT / ICS side
- [ ] Considering it on the OT / ICS side
- [ ] Currently sharing OT / ICS threat information with CISA
- [ ] Would consider sharing anonymous OT / ICS threat information with CISA
- [ ] Not considering OT / ICS cybersecurity monitoring because it is too costly
- [ ] Not considering OT / ICS cybersecurity monitoring because we have other security priorities
- [ ] Not considering OT / ICS cybersecurity monitoring because we are not technically ready for it yet
- [ ] Not considering OT / ICS cybersecurity monitoring because we do not have enough staff to add another project
- [ ] Not considering OT / ICS cybersecurity monitoring because we do not see a net benefit
- [ ] No
- [ ] Not sure
- [ ] Other (please specify)

17. If you are using an ICS/OT cybersecurity monitoring solution, would your utility be willing to be part of an anonymous study to help the sector better understand the costs and benefits of ICS/OT cybersecurity monitoring? If you are, please provide contact information and WaterISAC will follow-up with you or email hildick-smith@waterisac.org separately. It will take approximately a half hour of time and cover topics like installation and maintenance costs, alarm frequency and accuracy, technical skills required, and benefits.

- ◯ Yes
- ◯ No

Contact information

18. Has your utility evaluated your water or wastewater process for critical systems or equipment that might be vulnerable to physical damage from a cyber-attack?

- ◯ No
- ◯ No, but we plan to
- ◯ Yes, we have looked into it and found no vulnerabilities
- ◯ Yes, we have looked into it and found possible vulnerabilities
- ◯ Yes, we have looked into it and are considering installing cyber-physical safety systems to mitigate risk (e.g. changing valve gearing to prevent water hammer, etc.)
- ◯ Yes, we have looked into it and have installed cyber-physical safety systems to mitigate risk (e.g. changing valve gearing to prevent water hammer, etc.)
- ◯ Not sure
- ◯ Other (please specify)

19. What type of cybersecurity project did your utility most recently complete and what is up next?

Recent

Next

Anonymous Cybersecurity Survey for U.S. Water and Wastewater Utilities

Cybersecurity Education and Resources Used

20. In the last 12 months or so, what webinars, classes, events or workshops have staff attended for learning about IT and OT cybersecurity? Select all that apply.

- [ ] WaterISAC Threat Briefings and other webcasts
- [ ] EPA Introduction to Cybersecurity workshops
- [ ] AWWA classes
- [ ] MS-ISAC webcasts
- [ ] Vendor classes
- [ ] FedVTE classes
- [ ] Online classes from Coursera, EdX, etc.
- [ ] Cybersecurity conferences
- [ ] Cybersecurity organization classes from SANS, Infosec Skills, etc.
- [ ] None
- [ ] Not sure
- [ ] Other (please specify)

21. What free cybersecurity services has your utility taken advantage of or is planning to take advantage of? Select all that apply.

- [ ] DHS CISA Cyber Hygiene Vulnerability Scanning
- [ ] DHS CISA Phishing Campaign Assessment
- [ ] DHS CISA Cybersecurity Evaluation Tool (CSET)
- [ ] DHS CISA Cyber Resilience Review (CRR)
- [ ] DHS CISA Cyber Infrastructure Survey
- [ ] DHS CISA Validated Architecture Design Review (VADR)
- [ ] U.S. EPA Risk Assessment
- [ ] CIS / MS-ISAC Malicious Domain Blocking and Reporting (MDBR)
- [ ] CIS / MS-ISAC Malicious Code Analysis Platform (MCAP)
- [ ] None
- [ ] Not sure
- [ ] Other (please specify)

Anonymous Cybersecurity Survey for U.S. Water and Wastewater Utilities

Wish List

22. What help does your utility need to maintain or improve cybersecurity? Select **your top 3**. Feel free to add additional ideas.

- [ ] Advice on where to start
- [ ] Technical assistance, advice, assessments, or other "hands on support"
- [ ] Federal grants or loans for cybersecurity equipment or services
- [ ] Training and education targeting the water and wastewater sector
- [ ] Assurance of supply chain integrity of IT and OT hardware and software
- [ ] Funding to hire cybersecurity personnel
- [ ] Help finding cybersecurity personnel
- [ ] Cybersecurity threat information
- [ ] No assistance is needed
- [ ] Not sure
- [ ] Specific services, specific guidance, or other (please specify)

23. WaterISAC holds monthly Cyber Threat Webinars and occasional topical webinars. What topics would you be interested in seeing? Select **your top 5**.

- [ ] Management oriented topics
- [ ] Technically oriented topics
- [ ] Information about standards/guidelines and frameworks
- [ ] More threat information
- [ ] Access control and passwords
- [ ] Asset identification and inventory
- [ ] Endpoint detection and response (EDR)
- [ ] ICS cybersecurity monitoring
- [ ] Patching
- [ ] Secure remote access
- [ ] Vulnerability assessments
- [ ] Phishing and social engineering

- [ ] Segmentation
- [ ] Backups and restoration
- [ ] Data encryption at rest and in transit
- [ ] Policies and procedures
- [ ] Aspects of cybersecurity leadership
- [ ] Manual operations
- [ ] Logging
- [ ] Baseline memory capture
- [ ] Forensics
- [ ] Cyber-physical safety systems / engineered risk mitigation
- [ ] Cybersecurity funding sources
- [ ] Wireless security
- [ ] Incident response
- [ ] Physical security
- [ ] Awareness training and culture
- [ ] Process review and improvement
- [ ] Table-top exercises
- [ ] Process and control element isolation
- [ ] PLC security
- [ ] SCADA/ICS test bench
- [ ] Incident reporting
- [ ] Threat hunting
- [ ] Independent monitoring system
- [ ] USB thumb drive security
- [ ] Multi-factor authentication
- [ ] Change management
- [ ] Cloud security
- [ ] OT and cloud services
- [ ] Penetration testing
- [ ] Virtualization
- [ ] Host identity protocol
- [ ] Software defined perimeter
- [ ] Data Diodes
- [ ] Application control
- [ ] Security metrics
- [ ] Asset hardening
- [ ] Software supply chain risk

- [ ] Software bill of materials (SBOMs)
- [ ] Operations Security (OpSec)
- [ ] Open-Source Intelligence (OSINT)
- [ ] Zero Trust architecture
- [ ] Data loss prevention (DLP)
- [ ] Cybersecurity Maturity Model Certification (CMMC)
- [ ] Procurement security
- [ ] Not sure
- [ ] Other (please specify)

24. Other comments and suggestions?