WATER ISAC

2025 Q4

INCIDENT REPORT SUMMARY

Cybersecurity Incidents

CYBERSECURITY SUMMARY

- **8%** of respondents reported at least one cybersecurity incident. Industrial Control Systems (ICS) were involved in **34%** of incidents, followed by phishing and social engineering (**31%**) and ransomware (**23%**).
- While no members reported **ransomware attacks** directly, partner and open-source reporting indicate it remains a significant threat.

- **Supply chain risks** also persisted, with vendor-related incidents impacting operations.

Key developments included:

- Sustained hacktivist targeting of water sector ICS/OT systems, with pro-Russia groups claiming intrusions and leveraging unverified access for propaganda and influence operations.
- Attackers accessed a water treatment honeypot (a decoy network) and breached simulated HMIs, PLCs, and industrial protocols demonstrating exploitation of water system OT environments.
- A ransomware attack on the CodeRED notification platform disrupted emergency alerting capabilities at municipalities in several states.

Physical Security Incidents

PHYSICAL SECURITY SUMMARY

- **15%** of respondents reported at least one physical security incident this quarter.
- **Sabotage and tampering** were the largest incident category this quarter, including vandalism and copper theft that caused operational disruptions.

- **Insider threats** also remained a concern, with employee fraud and theft reported.
- Two **assault incidents** occurred, including one resulting in the deaths of two utility workers.

Notable incidents included:

- A disgruntled employee tampering with treatment system controls to disrupt operations.
- An individual arrested for deploying an improvised explosive device targeting manhole infrastructure.

- Multiple arrests tied to copper wire and diesel thefts that damaged pump stations.
- A suspected murder-suicide involving two utility employees.
- Fiber optic cuts that significantly disrupted wastewater utility operations.