WATER ISAC

2026 Q1 INCIDENT REPORT SUMMARY

Cybersecurity Incidents

CYBERSECURITY SUMMARY

5% of respondents reported at least one cybersecurity incident during the reporting period.

- **36%** involved **industrial control systems (ICS)**, including utility-reported operational technology (OT) incidents and numerous hacktivist claims targeting water infrastructure.
- **Social engineering and phishing continued to grow in sophistication.** Several utilities noted employee awareness training and email security controls successfully prevented compromise despite increasingly sophisticated phishing attempts.
- **Ransomware continued to heavily target organizations that support the water sector**, including engineering firms, chemical suppliers, and other organizations that provide products or services to utilities.
- **Third-party and supply-chain risk remained prominent**, with vendor compromise and service-provider outages creating downstream impacts for utilities.

Most notable cyber incidents or activity for the reporting period:

- Utilities reported multiple unauthorized access incidents involving remotely deployed OT/ICS assets, including one incident that resulted in a minor operational disruption.
- A drinking water utility discovered a former employee had retained sensitive supervisory control and data acquisition (SCADA) plans, diagrams, and schematics, highlighting insider threat risks.
- Hacktivist groups continued claiming access to water and wastewater control systems worldwide, demonstrating sustained interest in water-sector ICS and the use of alleged intrusions for propaganda and influence operations.
- A ransomware attack affecting a North Dakota water treatment plant's SCADA environment required approximately 16 hours of manual operations during recovery.
- A third-party payment processor, BridgePay, was the victim of a ransomware attack that disrupted utility billing and online payment services for municipalities and utilities in several states.

Physical Security Incidents

PHYSICAL SECURITY SUMMARY

5% of respondents reported at least one physical security incident during the reporting period.

- **Theft** was the largest tracked incident type, with copper theft and employee theft representing a large share of the incidents.
- **Surveillance or suspicious questioning** incidents that suggested threat actors were conducting pre-operational surveillance against water and wastewater utilities.
- **Sabotage/tampering** incidents that caused major operational impacts.

Most notable physical security incidents or activity reported this quarter:

- A sabotage/tampering incident involving a domestic violent extremist, in what law enforcement say was a targeted "terrorism-related event."
- A vandalism incident at an electric substation caused an oil leak, contaminating nearby waterways that feed into a small combined utility's water system. Due to the risk of contamination, authorities issued a "Do Not Consume" water advisory that remained in effect for over a month.
- At a large drinking water utility, workers were doing routine maintenance in a residential area when they encountered a man who threatened to shoot them with a rifle.