WATER ISAC

2025 Q1
INCIDENT REPORT SUMMARY

Cybersecurity Incidents

CYBERSECURITY SUMMARY

19% Of respondents reported at least one cybersecurity incident during the reporting period. Notable details of anonymized reports are presented below.

Top Types of Cyber Incidents Reported

- **26%** involved **Industrial Control Systems**
- **55%** involved a social engineering component, often leading to system compromise
- This quarter's reported incidents saw a significant rise in distributed denial-of-service (DDoS) attacks

Hacktivisim Continues to be a Prevalent Threat

- Russian Affiliated Group, Z-Pentest Alliance appeared again this quarter
- Several lone-wolf hacktivist attacks
- False claims and extortion attempts caused disruptions

Most notable cyber incidents or activity for the reporting period:

- The Russian-affiliated hacktivist group Z-Pentest Alliance posted an 11-second video to Telegram to demonstrate alleged compromise of an industrial control system interface.
- An employee from a third-party engineering firm that had a contractual relationship with a medium-sized wastewater utility, reported to WaterISAC partners that it suspected the utility's wastewater controls system was compromised.
- Multiple threat actors operating under various aliases posted to the dark web claiming to have compromised OT systems at different water utilities, sometimes advertising compromised credentials.
- A large drinking water utility was impacted by the Cityworks exploitation that occurred in early February. WaterISAC sent an **advisory** to members on February 3rd regarding incidents in the water and wastewater sector resulting from vulnerabilities in Cityworks software.
- A very large, combined utility identified a typosquatting attack where four lookalike domains closely resembled its official domain.

Physical Security Incidents

PHYSICAL SECURITY SUMMARY

22% Of respondents reported at least one physical security incident during the reporting period. Notable details of anonymized reports are presented below.

- **Theft** continues to be the highest reported threat
- **Sabotage** incidents continue to be reported, leading to operational impacts
- **Threat of Harm**
  - Bomb threats
  - Threats of poison
  - Assault and threats of harm against utility workers

Most notable incidents or activity reported this quarter:

- Two cases of bomb threats directed at water and wastewater utilities. In one case, a former disgruntled utility employee was charged by law enforcement for allegedly making a bomb threat at the utility and for threatening to poison the utility's water supply.
- A sabotage/tampering incident where unknown perpetrator(s) tampered with two fire hydrants, which led to approximately 30,000 liters of untreated sewage leaking into a nearby major river.
- Two incidents involved threats to poison a utility's water supply, including one where a suspect was charged with domestic terrorism.