

Cybersecurity Incidents

CYBERSECURITY SUMMARY

11% of respondents reported at least one cybersecurity incident during the reporting period.

Top Types of Cyber Incidents in the Report

- **18% involved Industrial Control Systems (ICS)**, including utility-reported, hacktivist claims, and open-source disclosures of OT-focused incidents.
- **Ransomware** remained the largest tracked incident type, with most claims targeting suppliers, contractors, and service providers that support the water sector rather than utilities themselves.
- **Iran-linked activity** against U.S. water systems included a CISA-reported targeting attempt against a utility and a hacktivist claim of stolen customer billing data from a large water utility.
- **Credential-based attacks**, such as password spraying and brute-force methods against remote access appliances and control interfaces, also featured in several OT-related incidents and claims.

Most notable cyber incidents or activity for the reporting period:

- ⚠️ A claimed breach of a large California water utility by the Iran-linked Handala group, which published customer billing data and credentials for an internal GPS correction network that researchers assessed as a likely pathway into the billing environment.
- ⚠️ An AI-assisted intrusion in which an adversary who had compromised a Mexican water utility's enterprise network used commercial AI models to identify an OT-adjacent gateway and attempt password spraying against it, although no OT access was gained.
- ⚠️ An incident in which a threat actor used a compromised account to impersonate a water sector organization's hiring manager on job sites, collecting resumes and potentially sensitive personal information from approximately 200 applicants.

Physical Security Incidents

PHYSICAL SECURITY SUMMARY

14% of respondents reported at least one physical security incident during the reporting period.

- **Theft** remained the largest tracked incident type, similar to last quarter, with copper theft representing the largest share of incidents.
- **Threat of harm** incidents and one **assault** against utility workers in the field highlighted the heightened threat of workplace violence that water and wastewater sector employees face.
- **Sabotage/tampering** incidents led to significant operational impacts, including disruptions to drinking water and firefighting services.

Most notable physical security incidents or activity reported this quarter:

- ⚠️ A sabotage/tampering incident where a petty criminal was arrested and charged for reportedly vandalizing a drinking water pump station, which caused a temporary loss of water service for 84 homes.
- ⚠️ A vandalism and major burglary incident at a small drinking water utility that caused significant damage to its water treatment plant, which temporarily rendered parts of the facility inoperable and disrupted water service to the local community.
- ⚠️ An incident at a very large combined utility in which contracted divers discovered what appeared to be a grenade near the gate of a dam for a reservoir.