WATER ISAC



Threat Analysis for the Water and Wastewater Sector

Incidents, suspicious activities, threat assessments, and predictions.

EXECUTIVE SUMMARY

November 2026

TLP:CLEAR

Background

About WaterISAC

The Water Information Sharing and Analysis Center (WaterISAC) is the designated information sharing and operations arm of the Water Sector Coordinating Council (WSCC). WaterISAC helps utilities in the U.S., Canada, Australia, and New Zealand measure and reduce risk, improve resiliency, prepare for physical and cyber threats, and recover from disasters.

WaterISAC members have access to the world's largest and richest source of information and tools for strengthening water and wastewater utility security, preparedness, resilience, and emergency management.

WaterISAC also supports federal, state, and local government agencies involved in water resources, law enforcement, emergency response, intelligence, and public health to inform programs and initiatives to protect critical infrastructure and public health.

WaterISAC is a non-profit organization created in 2002 by utility managers and is governed by a board appointed by the leading national water and wastewater organizations.
To log in to WaterISAC's secure portal, go to **www.waterisac.org**.

Scope

The *Threat Analysis for the Water and Wastewater Sector* provides WaterISAC's assessments and predictions of threats facing the water and wastewater sector in terms of physical security, natural disasters, and cybersecurity. This report does not include summaries of all the incidents and suspicious activities that have recently been reported by members or observed by WaterISAC. Descriptions of physical security and cybersecurity events are provided in WaterISAC's *Quarterly Water Sector Incident Summary* reports. However, the analysis provided in this document is informed by the most recent *Quarterly Water Sector Incident Summary* reports. Members can access these and other WaterISAC reports on the **WaterISAC Publications** webpage of WaterISAC's portal.

The analysis in this document is solely the product of WaterISAC and does not necessarily reflect the views of other entities. The events analyzed in this document should not be considered a comprehensive data set of all incidents and suspicious activities that occurred in the water and wastewater sector. However, they do provide insights into the types of incidents occurring at sector assets and the threats they may encounter.

Executive Summary

Cybersecurity Threat Landscape

The cybersecurity threat landscape facing water and wastewater utilities continues to evolve, shaped by an expanding set of adversaries, rapidly advancing technology, and sustained geopolitical conflict. While cybercrime still dominates the landscape by sheer volume, the past year brought a marked escalation in threats directed at operational technology (OT) and industrial control systems (ICS), including **some of the most significant coordinated attacks on U.S. water utilities the sector has yet seen**.

Key Cybersecurity Trends and Activity:



- **Hacktivism has become a defining threat to OT.** Fueled by geopolitical conflict, hacktivist groups—many state-sponsored or state-aligned—have expanded beyond website defacements and distributed-denial-of-service (DDoS) campaigns toward claimed data leaks and disruption of cyber-physical systems. Research consistently identifies water utilities as one of the most targeted sectors for hacktivist activity, although a large share of these claims remain unverified and should be read as signals of intent and threat actors' interest rather than confirmed compromise.
- **Threat actors produced real operational effects at U.S. water utilities.** In late July 2026, a coordinated campaign against internet-exposed programmable logic controllers (PLCs) struck more than 100 water systems across at least 12 states, locking out operators and, in some cases, causing water pressure to drop. While Iran-linked actors are as suspected of being responsible for the attacks, formal attribution remains pending.



- **Artificial intelligence (AI) is reshaping the threat environment.** AI is lowering the cost and raising the quality of the social-engineering attacks that already dominate members' incident reports—AI-written phishing is measured as roughly 4.5 times more effective than human-written—while controlled testing has shown AI agents capable of compressing the path from network access to physical effects in OT environments to a matter of minutes.
- **Nation state and supply chain threats carry the highest potential impact.** Chinese "Typhoon" actors continue pre-positioning within critical infrastructure and, in at least one case, sought to exfiltrate OT operating data. A Russia-aligned group conducted a coordinated attack on Poland's power grid with direct parallels to water-sector architecture. Third-party compromises—from billing platforms to notification services—repeatedly cascaded into utility operations from a single point of failure.



Physical Security Threat Landscape

The physical security threat environment for water and wastewater utilities is volatile and will likely remain elevated into 2027. Utilities are attractive targets to a diverse set of actors because the sector is a lifeline for every other infrastructure sector and is essential to public health. The report identifies six drivers heightening the threat landscape: cyber-physical convergence, geopolitical conflict, political polarization, growth in destructive anti-social behavior, financial opportunity for criminals, and the sector's role in supporting other critical infrastructure. Cyber-physical convergence means that weak physical security can undermine cybersecurity, and that compromised operational technology can cause physical consequences. In addition, utility workers face rising threats and violence from disgruntled customers and from extremists who view them as extensions of government.

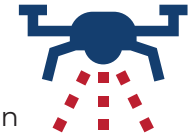
Key Physical Security Trends and Activity:

- **Physical security threats remain elevated.** WaterISAC recorded 46 sabotage and tampering incidents from Q2 2025 through Q1 2026, a 44% increase over the prior four quarters. Theft remained the most frequently tracked event type. Online threats against the sector also rose sharply, with at least 20 in 2025 (up from five in 2024) and more than 25 in the first half of 2026 alone.

- **Several threat categories are intensifying.** Geopolitical conflict, particularly the U.S.-Iran war and Russia's hybrid sabotage campaign in Europe, has normalized attacks on water infrastructure. Hostile nation states (Russia, China and Iran) have significantly increased their physical threat to the sector, and insider recruitment is a growing concern. Violent extremists across the ideological spectrum remain a lethal threat and continue to target critical infrastructure.



- **Emerging technologies are widening the attack surface and lowering barriers for adversaries.** Drones are increasingly used for hostile surveillance and as explosive-laden weapons. AI is being exploited by violent extremists and other threat actors to facilitate attack planning, amplify propaganda, conduct reconnaissance, and generate disinformation that is increasingly difficult to detect.



- **Common criminals remain the most persistent threat and the most likely to impact utilities.** Rising copper prices, remote and hard-to-secure assets, and resource constraints make utilities appear to be soft targets, and thefts and vandalism have caused significant financial and operational disruption. Opportunistic actors without clear motives are also increasingly damaging remote infrastructure assets.



Natural Hazards Threat Landscape

Compared to last year, when catastrophes like hurricanes Helene and Milton and the Eaton and Palisades fires were still in recent memory, the previous months seem relatively tame. A closer examination reveals significant activity across key natural disaster areas. These events demonstrate the water and wastewater sector continues to confront a diverse and challenging array of such threats, which have been exacerbated by climate change.

Key Natural Disaster Trends and Activity:

- **Severe storms and flooding often represent one of the greatest natural disaster threats to water and wastewater utilities.** Flooding remains the most frequent and costliest U.S. natural disaster. The U.S. has largely been spared the last two years from one of its greatest contributors: landfall-making hurricanes. That does not mean there hasn't been significant tropical storm activity, as 2025's Hurricane Melissa and a series of systems affecting Hawaii this year attest. A "super El Niño" has not only had a major influence on activity in the Atlantic and Pacific, but it has also influenced weather patterns and the other natural disaster categories.

- **Drought concerns made national news, especially when the U.S's first and second-largest reservoirs recorded their lowest water levels in their decades' long history.** Drought affected more than just the West and Southwest, given reports in April of one of the most widespread and intense droughts in decades, with over 60% of the country affected. According to a recent U.S. Drought Monitor report, drought conditions across the country present "a mixed bag."

- **Wildfires represented an especially active category, with the last year experiencing the greatest number of fires and acres burned over the last ten years.** In 2026, there have been nearly 69,000 fires that have altogether burned approximately 9.5 million acres. The Spokane Complex was among these disasters; it burned approximately 11,000 acres and caused significant impacts in the water and wastewater sector. Earth's warming climate is contributing to these disasters, through increasingly dry air, vegetation, and soils that make it easier for fires to spread and harder to fight or prevent.

- **Extreme temperatures not only contribute to other disasters, they represent their own category of disaster.** Extreme heat has been the greatest weather-related cause of death in the U.S. for the past 30 years, necessitating that utilities consider employee safety when temperatures are elevated. They should also be mindful of how extreme temperatures affect infrastructure and operations and the effects of extreme cold, especially with the approach of winter.



Supply Chain Risk for the Water and Wastewater Sector

Water and wastewater utilities face supply chain disruptions from many sources, including malicious activity, overreliance on specific suppliers, and supplier failures, among other contingencies. Recent examples include COVID-19 chemical shortages, energy price spikes from the Russia-Ukraine war, a chemical plant fire, transportation strikes, and the current U.S.-Iran conflict.

Chemical supply is a critical vulnerability because the sector depends on a small set of treatment chemicals, with chlorine production concentrated among few manufacturers. Equipment supply chains are also at risk: PLCs, remote terminal units (RTUs), and supervisory control and data acquisition (SCADA) hardware come from a limited number of manufacturers, creating single points of failure, and counterfeit components have entered utilities, as shown by a counterfeit PLC found during a pump-station upgrade.

Other Critical Infrastructure Lifelines – Physical Security Threats

The energy, communications, and transportation sectors, on which water and wastewater utilities depend for power, equipment monitoring, and the movement of chemicals and other materials, face an evolving physical security threat environment in which a disruption to any one sector can cascade to water utilities even when they are not directly targeted.

In the electric sector, physical security threats to the power grid remain a significant concern. Threat actors are primarily driven by economic and criminal motives, including high copper prices. Notably, grid-impacting incidents increased in 2025 compared to 2024, with the January 2026 arson attack in Berlin illustrating the elevated threat. In the communications sector, theft and vandalism incidents exceeded 18,000 in 2025, a 59% increase, compared to 2024, which disrupted service for nearly 12 million customers, with insider threats also a growing concern. In the transportation sector, cargo theft losses reached nearly $725 million, a 60% increase, and rail infrastructure continues to be an attractive target for violent extremists and hostile nation state operatives.





WATER ISAC

1250 I Street, NW, Suite 350
Washington, DC 20005
1-866-H2O-ISAC (1-866-426-4722)
waterisac.org