TLP:CLEAR

Q1 2026

Water & Wastewater Sector

A Quarterly National Security Information-Sharing Bulletin from the U.S. Environmental Protection Agency and the Water Information Sharing and Analysis Center

In This Issue

Please take this short survey to share your feedback and help improve the quarterly bulletin.

Click Here to Share Your Feedback!

Ransomware State of Play and the National Security Implications

Ransomware and extortion continued to be widely regarded by the U.S. government and leading cybersecurity firms as one of the most significant and pervasive cybersecurity threats to critical infrastructure in 2025. There were at least 7,419 ransomware attacks recorded worldwide in 2025, representing a 32% increase over the 5,631 attacks recorded in 2024. Of those attacks, the U.S. was the most heavily targeted nation with approximately 3,810 attacks on U.S. entities, according to research from the cybersecurity firm Comparitech.

Ransomware attacks against water and wastewater utilities are often framed as costly IT incidents, but their implications extend far beyond financial loss or business disruptions. Ransomware attacks on the water sector, and critical infrastructure writ large, should be considered a national security threat because these attacks can directly undermine a nation's ability to function, protect its population, and respond to crises.

The water sector provides essential services that directly impact public health, community stability, and economic activity. An attack that compromises treatment processes, monitoring systems, or billing platforms can erode public trust and, in worst-case scenarios, threaten the safety of drinking water or the proper handling of wastewater. When these systems are disrupted, even temporarily, the consequences can cascade across sectors, causing widespread harm that extends far beyond financial loss.

Ransomware attacks are increasingly linked to sophisticated criminal groups and, in some cases, to state-aligned actors, blurring the line between crime and geopolitical coercion. This creates opportunities for adversaries to weaken national resilience, sow public distrust, and exert pressure without engaging in traditional military conflict.

Ransomware and extortion are disproportionately impactful on critical infrastructure entities because they strike directly with how infrastructure systems are built, operated, regulated, and funded. For sectors like energy, water, and transportation, ransomware exploits structural weaknesses that other threats do not monetize as effectively. For instance, most critical infrastructure sectors prioritize continuous operations; water must flow, power must stay on,

Continues on page 2

hospitals must deliver care, manufacturing lines must not stop. Ransomware attacks seek to disrupt business continuity and operational availability. Based on multiple cybersecurity reports and incident data from law enforcement sources, detailed below are the top 5 ransomware variants/groups that impacted critical infrastructure sectors in 2025, including the water and wastewater sector:

Qilin: Qilin is a financially motivated threat actor group that has operated as a ransomware-as-a-service (RaaS) model since at least June 2022. Its affiliates usually gain initial access through compromised VPN credentials and then conduct post-compromise activity using legitimate tools as well as commodity, open-source, or custom malware. They commonly use a double-extortion strategy—stealing sensitive data before encrypting networks—and may also apply pressure through extortion calls, DDoS attacks, or legal threats.

Akira: The Aikira group developed and maintains the Akira ransomware and its associated Akira dedicated leak site (DLS). The Tactics, Techniques, and Procedures (TTPs) associated with Akira ransomware deployments include significant use of legitimate repurposed software and open-source penetration-testing tools. Aikira relies on sensitive data exfiltration and encryption to extort ransom payments from victims. The attacker typically gains initial access through VPN appliances, historically, this has included exploitation of the ASA and FTD vulnerability CVE-2023-20269. Since August 2024, it has also used SonicWall SSLVPN connections for initial access.

Clop: Clop is a financially motivated threat actor group that uses Clop ransomware. The threat actor has published victim data from ransom campaigns to the "Clop Leaks" site. However, the Clop group has not deployed ransomware since late 2022 and instead has relied on data-theft and extortion campaigns. Specifically, the threat actor has exploited zero-day vulnerabilities, often with a focus on file transfer applications to steal data and extort victims with the stolen data.

Play: Play is a financially motivated threat actor group that first emerged in June 2022. The Play group developed and privately operates the PLAY ransomware. In addition to PLAY ransomware, Play uses custom discovery and defense evasion tools. They also deployed a downloader currently tracked as FrostbiteLoader.

INC: The INC financially motivated threat actor group has developed several ransomware variants, such INC and Lynx. With each new ransomware variant, INC retires the previous variant. Initially, INC targeted smaller organizations and demanded smaller ransom demands; however, the threat actor has encouraged its affiliates to target larger organizations for higher ransoms; affiliates have subsequently been using Big Game Hunting (BGH) tactics. BGH refers to a ransomware and extortion strategy where threat actors deliberately target large, high-value organizations rather than many small victims.

There are practical steps water utilities can take to significantly reduce their risk from ransomware attacks without requiring advanced technical capabilities or large budgets. Basic cyber hygiene measures—such as keeping systems patched, enforcing strong passwords and multi-factor authentication, segmenting operational technology from business networks, and maintaining regular, offline backups—can prevent the vast majority of ransomware attacks. Regular staff training to recognize phishing and social engineering attempts also further reduces risk, since many intrusions begin with simple human error.

Treating ransomware as a national security threat encourages a shift from minimal compliance toward proactive risk management, intelligence sharing, and coordination with government partners. It also reframes cybersecurity investment as a core responsibility tied to public safety and national resilience, rather than a discretionary cost. By adopting this perspective, owners and operators can better align their defenses with the scale of the risk and their role in protecting the broader national interest.

Additional Reading:

- Ransomware Threat Outlook 2025-2027
- The State of Ransomware in Enterprise 2025
- Top 10 Ransomware Groups of 2025

Mitigation Recommendations:

- EPA – Cybersecurity for the Water Sector
- CISA – Stop Ransomware

ASK THE EXPERT: Interview with Loudoun Water's Director of Operational Technology

Water and wastewater utilities face a rapidly evolving cyber threat landscape. Operators and network defenders must balance daily operational requirements with legacy systems, resource constraints, and an expanded attack surface. While guidance from vendors is valuable, some of the most practical insights come from those working on the front lines: operators who are navigating the same constraints, risks, and resource realities.

To help us understand these challenges and ways to mitigate them, we spoke with Andy Krapf, the Director of Operational Technology at Loudoun Water, in Ashburn, VA, to offer his perspective on cybersecurity best practices for the water and wastewater sector to help utilities drive down risk and ensure continuous, uninterrupted operations.

Q: What are some first steps you would recommend for utilities that are working on enhancing their cybersecurity posture?

A: My recommended "first steps" are straightforward. First, designate a person who is both responsible and accountable for the cybersecurity program. Since this may or may not be the same individual for IT and OT systems, it is vitally important that OT security measures be informed by knowledge of cyber-physical systems. Next, develop an understanding of the organization's risk landscape by asking these questions:

- Who are the key stakeholders?
- What business processes are most important to the company?
- What are the consequences of these processes being unavailable?
- Are there constraints to consider (safety, budget, resources, regulations)?
- What is the company's risk tolerance?

Finally, define reasonable, achievable goals. These might relate to training, asset visibility, reducing the attack surface, or implementing network segmentation. Remember, success isn't about boiling the ocean. Creating a plan that has obtainable goals that build upon each other is both demonstrable and defensible.

Q: What's the best advice you could give to help other utilities minimize exposure of their OT systems to the public facing internet?

A: Start by asking, "Why are systems connected to the internet?" Determining whether there is a legitimate business need that has gone unaddressed, or if "shadow IT" may be present will be a crucial step in determining appropriate actions. OT systems should be continuously monitored to identify asset data flows with particular scrutiny given to assets that are directly connected to the internet. It is important to challenge whether connectivity is necessary and disconnect those that are not. Governance must apply to both internal staff, systems integrators, and third-party vendors to ensure only authorized remote access is permitted. Finally, where remote access is required, implement a robust Secure Remote Access (SRA) solution that provides auditable control and visibility over who accesses OT systems.

Q: What do you do to help foster a cyber secure culture?

A: A cybersecurity culture starts at the top with leadership and communication. Involving stakeholders in the decision-making process builds understanding

Continues on page 4

Loudoun Water Campus

of business needs and the challenges posed by cyber threats. Regular engagement fosters an environment of "How can I help?" instead of "No." I also recommend integrating cybersecurity into other business processes such as procurement, vendor management, engineering, and HR. Cybersecurity isn't just a technology issue—it's a business execution issue.

Q: What's your procedure to develop and maintain an accurate inventory of assets? And how has it been useful in your cybersecurity efforts?

A: Developing and maintaining an asset inventory can look very different depending on a utility's structure, size, and maturity. For networks that contain OT assets, it is paramount that technology specifically designed for OT is deployed. Many IT tools can cause disruptions or worse when used in OT networks. I strongly recommend using a network monitoring tool that automatically creates an inventory of assets. This can be entirely passive or combine active and passive discovery. The cybersecurity market offers many vendors with tools for utilities of all sizes, though they come with varying costs. Smaller organizations may use spreadsheets as a low-cost alternative. Once the inventory is established, utilities must act on the findings—eliminating shadow IT, addressing obsolete systems, and leveraging visibility to strengthen other programs. Asset visibility can serve as the foundation for Patch Management, Backup and Restoration, and Lifecycle Management programs. It also helps enforce device standards and consistent infrastructure design.

Q: When you urgently need to patch an OT system, but are unable to due to business needs, how do you go about implementing compensating controls?

A: When urgent patching is required, the first step is to evaluate the potential operational impact. Where redundancy exists, patching becomes less disruptive if properly planned. For OT systems like PLCs, close coordination with Operations is critical to minimize downtime. If applying a patch immediately is not possible, we increase monitoring and apply additional scrutiny using a variety of tools to detect anomalies quickly. It is also important to reference the CISA Known Exploited Vulnerabilities (KEV) catalog to determine whether the exploit has been observed in active use.

Q: How important is logging and monitoring to your cybersecurity program?

A: Logging and monitoring are essential to any cybersecurity program. Most environments monitor north–south network traffic (into and out of the network), but it is equally important to monitor east–west traffic within the network. A robust monitoring system can detect abnormal communication between devices. Windows Event Logs, application logs, network device Syslogs, and SNMP messages all help create a holistic view of system health. These logs should drive alerts, dashboards, reports, and performance metrics, and ultimately improvements across monitored networks.

Q: How useful is your incident response plan (IRP)? How important is it for utilities to develop and follow an IRP?

A: Having an incident response plan (IRP) is a cornerstone of a mature cybersecurity program. IRPs provide responders with structured guidance and help maintain focus during high-stress situations. They also prevent critical steps from being overlooked during a crisis. More important than simply having a plan is regularly testing and exercising it. Utilities should periodically conduct simulated incidents using their IRP to verify that documentation, procedures, and participant understanding remain current.

Incident Response Plans are not constructed just to sit on a shelf or file server; they have to be reviewed, tested, and refined. As new threats and capabilities arise, our IRPs must evolve.

Hacktivists Activity Targeting Critical Infrastructure Surged in 2025, Likely to Remain a Significant Threat in 2026

Over the past several years, hacktivists groups, specifically pro-Russia hacktivists, have been observed conducting cyber attacks against numerous organizations and critical infrastructure sectors worldwide. These activities grew significantly in 2025, alongside the increased targeting of industrial control systems (ICS). Due to this heightened threat, water and wastewater utilities are strongly encouraged to prioritize securing their operational technology (OT) using the mitigation guidance at the end of this report.

Multiple cybersecurity firms and researchers have highlighted the increasing tempo of hacktivists attacks against water and wastewater utilities. For example, in a Forescout Report "The Rise of State-Sponsored Hacktivism", which analyzed 780 hacktivist attacks in 2024, water utilities made up the largest group targeted. This trend continued into 2025 according to a recent report "Critical Infrastructure Attacks Became Routine for Hacktivists in 2025" from the cybersecurity firm Cyble.

In 2025, "hacktivists moved well beyond their traditional DDoS attacks and website defacements in 2025, increasingly targeting industrial control systems (ICS), ransomware, breaches, and data leaks, as their sophistication and alignment with nation-state interests grew," according to the report. Indeed, hacktivism has developed into a geopolitically charged, ICS-focused threat, continuing to exploit exposed OT environments. Cyble observed a 51% increase in hacktivist sightings in 2025, with multiple, primarily pro-Russia groups, increasing their focus on ICS and OT attacks.

The report noted that "Human Machine Interfaces (HMI) and web-based Supervisory Control and Data Acquisition (SCADA) interfaces were the most frequently targeted systems, followed by a limited number of Virtual Network Computing (VNC) compromises, which posed the greatest operational risks to several industries." Hacktivists have also been observed increasingly using AI-generated text and imagery for propaganda and spreading misinformation and disinformation.

Additionally, an advisory published in January by the UK's National Cyber Security Centre, "**Pro-Russia hacktivist activity continues to target UK organisations**," said that in 2026 pro-Russia hacktivists are continuing to target the UK and international entities by attempting to disrupt operations, take websites offline and disable services. Going forward, Cyble's experts assess that hacktivists and cybercriminals will increasingly target exposed

HMI/SCADA systems and VNC takeovers, aided by public PoCs and automated scanning templates.

Recommended mitigation actions that will help reduce organizational reduce risk include, but are not limited to:

- Reduce exposure of OT assets to the public-facing internet.
- Adopt mature asset management processes, including mapping data flows and access points.
- Ensure that OT assets are using robust authentication procedures.

Read the full hacktivist report here.

Additional Reading:

- **The Rise of State-Sponsored Hacktivism**

Mitigation Recommendations:

- **(TLP:CLEAR) CISA and Partners Release Secure Connectivity Principles for Operational Technology**
- **Defending OT Operations Against Ongoing Pro-Russia Hacktivist Activity**
- **Security considerations for industrial control systems**

INSIDER THREAT CORNER – Risk of Remote Exploitation

A significant counterintelligence problem facing the water and wastewater sector is the convergence of IT and Operational Technology (OT) networks, which has left unsecured, internet-facing critical infrastructure vulnerable to remote exploitation. Adversaries, including state-sponsored actors, cybercriminals, and malicious insiders exploit this, often targeting weak, outdated systems to disrupt water supplies or cause panic.

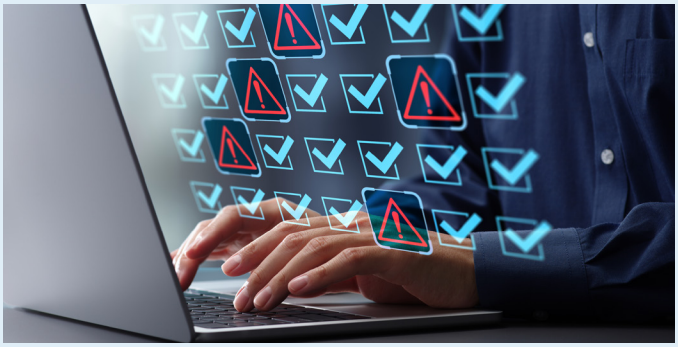
Key aspects of this vulnerability include:

- Insecure Remote Access & Weak Credentials: Many systems use default passwords and have uncontrolled, undocumented external connections.
- Lack of Segmentation: Poorly separated IT and OT networks allow attackers to move laterally from business systems into, critical, industrial control systems.
- Aging Infrastructure: The sector often relies on outdated, legacy equipment not designed with modern security, making them easy targets for disruption, such as tampering with chemical levels.
- High-Value Target: Adversaries target these systems for disruption or to exert geopolitical pressure, especially in the U.S.

Case Study: In June 2023, the Department of Justice charged a former employee of a private Massachusetts-based company who contracted with Discovery Bay to operate the town's wastewater treatment facility installed software on his personal computer and the company's internal network that allowed him to gain remote access into the water treatment facility's computer network after he resigned. The employee was responsible for maintaining the instrumentation and the computer systems used to control the electromechanical processes of the facility in Discovery Bay. After the employee departed the company in 2021, he accessed the facility's computer system remotely and transmitted a command to uninstall software in the main hub of the facility's computer network that protected the entire water treatment system, including water pressure, filtration, and chemical levels.

Threat Type:

- Malicious Insider: A trusted person who intentionally misuses their authorized access to steal data, disrupt operations, or cause financial or reputational harm to their organization, often driven by financial gain, revenge, or ideology.



Incident Category:

- Cyber with elements of theft and sabotage because the employee stole the software to download on his personal computer, then used it to transmit commands that protected Discovery Bay's water treatment system, water pressure, filtration, and chemical levels.

Motivation:

- While the employee's exact motives were not explicitly detailed in public records, his actions occurred shortly after his contract ended, suggesting an intentional disruptive act against his former employer.

Indicators:

- The employee installed software on both his personal computer and the utility's private internal network.
- The employee used unauthorized remote access to gain access to the utility's computer network.

Outcome/Impact:

- The employee was charged for accessing Discovery Bay's computer network and shutting it down. He spent 6 months in home confinement, followed by 36 months of probation, had to forfeit his computer and paid $44,250 in restitution. The employee's actions were deliberate and intended to cause operational disruptions, posing a possible risk to the health and safety of the community's water supply.

Read more about Insider Threat Mitigation at CISA.

Additional Reading:

- Tracy Resident Charged With Computer Attack On Discovery Bay Water Treatment Facility
- Former contractor accused of remotely accessing town's water treatment facility

Authorities Disrupt Islamic State Ricin Plot in India that Planned to Poison Local Water Supplies

The risk of violence from foreign terrorist organizations (FTOs) and homegrown violent extremists (HVEs) against the U.S. and other Western countries remains elevated driven by several factors, such as the spread of emerging technology and ongoing geopolitical conflicts that have facilitated homegrown radicalization. The 2025 New Year's Islamic State-inspired attack in New Orleans, that caused over a dozen deaths, highlights the elevated threat.

FTOs, like the Islamic State, seek not only to conduct mass casualty attacks, but also to target critical infrastructure services to cause societal disruption, economic harm, and psychological fear rather than just casualties alone. Consequently, in November 2025, Indian authorities disrupted a terrorist plot to poison local water supplies, arresting three individuals with confirmed links to the Islamic State Khorasan Province.

In the past, malicious threat actors have attempted to use biological and chemical agents to target the water and wastewater sector. In 2018, for example, a Wisconsin based woman was charged with supporting the Islamic State by encouraging online supporters of the group she was in contact with to poison local water reservoirs with ricin. Before that, in 2015, Islamic State operatives plotted to poison water supplies in the European country of Kosovo, underscoring the persisting desire of FTOs to target public drinking water to conduct mass-casualty attacks.

In the Indian plot, the accused terrorists reportedly planned to manufacture the highly toxic biological agent ricin and target water supplies, religious sites, and public areas in major Indian urban centers. The plot involved a multi-national operation directed by an external Islamic State Khorasan Province handler, who provided instructions and logistical support. Tactical gear, including firearms and ammunition, were smuggled over the border from Pakistan via drone. One of the alleged terrorists converted his residence into a makeshift laboratory, acquiring precursor chemicals, castor beans, and an oil-press machine to manufacture the ricin.

Indian authorities reported that the individual responsible for manufacturing the ricin had not yet successfully isolated the toxin or determined a delivery mechanism at the time of his arrest. "This was not a case of lone-actor radicalization but a directed cell with a mature command-and-control structure. The presence of an external handler, transnational weapons smuggling, and a clear division of labor indicate a sophisticated network," according to a report by Indago Solutions.

The Islamic State-Khorasan Province remains one of the most lethal Islamic State affiliate groups with a network of transnational contacts and a persistent desire to conduct external operations in Western countries, such as the thwarted plot to attack a Taylor Swift concert in Austria. Ultimately, the Islamic State and al Qa'ida – based on their ability to inspire sympathizers in the West, which lowers the barrier to entry for targeted attacks – remain an enduring threat.

Read more here about the thwarted plot here.

Additional Reading:

- Nearing the End of 2025, What is the State of the Islamic State?
- A decade after the 'Caliphate': The state of the Islamic State online

Strengthening Water Infrastructure For Tomorrow

Natural disasters pose significant challenges to our Nation's drinking water, wastewater and storm water utilities, often resulting in infrastructure damage that disrupts the flow of critical services to our communities. It is critical that utilities account for these risks and make informed infrastructure planning decisions when recovering from previous disasters or preparing for the next one.

To advance EPA's national security mission to reduce water and wastewater utility risk from natural and malevolent acts, EPA has established a new initiative, Strengthening Water Infrastructure for Tomorrow (SWIFT), to support risk-informed project planning and investment decisions.

This approach focuses on increasing infrastructure resilience to natural hazards by providing direct technical assistance (TA) to individual utilities for risk assessments. SWIFT TA is tailored to meet the needs of each utility request, from improving the understanding of the threat that natural disasters pose to their system to quantifying the potential reductions in risk that specific projects could deliver. In addition, SWIFT provides workshops for utilities and stakeholders to learn through classroom style discussion. Workshops also build capacity for local and state agencies and TA providers to support communities using SWIFT resources.

With SWIFT support, utilities are better prepared to pursue available Clean and Drinking Water State Revolving Fund programs and Congressional Supplemental Funds to recover from and prepare for natural disasters. This support also assists water utilities with complying with requirements to conduct risk and resilience assessments and develop emergency response plans that must consider natural hazards and disasters.

To learn more about SWIFT, request TA, or view upcoming workshops, visit the SWIFT webpage: https://www.epa.gov/waterutilityresponse/strengthening-water-infrastructure-tomorrow-swift

TLP:CLEAR

Useful Links and Contact Information

For feedback, comments or questions related to the content in this bulletin, please email Water-NSISB@epa.gov

WaterISAC

- Website | www.waterisac.org/
- Membership Information | www.waterisac.org/membership
- Incident Reporting Form | www.waterisac.org/report-incident
- 24 Hour Line | 866-H2O-ISAC

EPA

- Office of National Security | www.epa.gov/national-security
- Drinking Water and Wastewater Resilience Website | www.epa.gov/waterresilience
- Cybersecurity for the Water Sector | https://www.epa.gov/cyberwater

Water Sector Coordinating Council

- American Water Works Association (AWWA)
- Association of Metropolitan Water Agencies (AMWA)
- National Association of Clean Water Agencies (NACWA)
- National Association of Water Companies (NAWC)
- National Rural Water Association (NRWA)
- Water Environment Federation (WEF)
- WaterISAC
- Water Research Foundation (WRF)