WATER & WASTEWATER SYSTEMS SECTOR CYBERSECURITY

Sector Overview

This resource is for stakeholders in Florida's Water and Wastewater Systems sector. It includes:

- Municipal water utilities
- Private water system operators.
- Regional water authorities and
- Wastewater treatment plants

The sector is essential to public health, environmental safety, and quality of life. A ransomware incident could cause public health emergencies or environmental hazards.

Ransomware Threat Profile

Fewer than 20% of Florida water and wastewater organizations meet DHS ransomware readiness standards. The sector faces high risk due to outdated infrastructure, limited cybersecurity staffing, and weak incident response capabilities. If compromised, these systems could disrupt water treatment and distribution, wastewater processing, and regulatory compliance.

Vulnerability Levels in U.S. Drinking Water Systems

(EPA Scan, 2024)

Risk Level	Number of	% of Sample	Population
Critical/ High	97	~9%	~26.6
Medium/ Low	211	~20%	~82.7
No Significant	754	~71%	Remainder

Note: Nearly 1 in 10 large U.S. drinking water systems were found to have critical cybersecurity vulnerabilities, affecting over 26 million people. Another 20% showed medium or low risks, signifying widespread gaps in cyber resilience across the sector.

Top Vulnerabilities

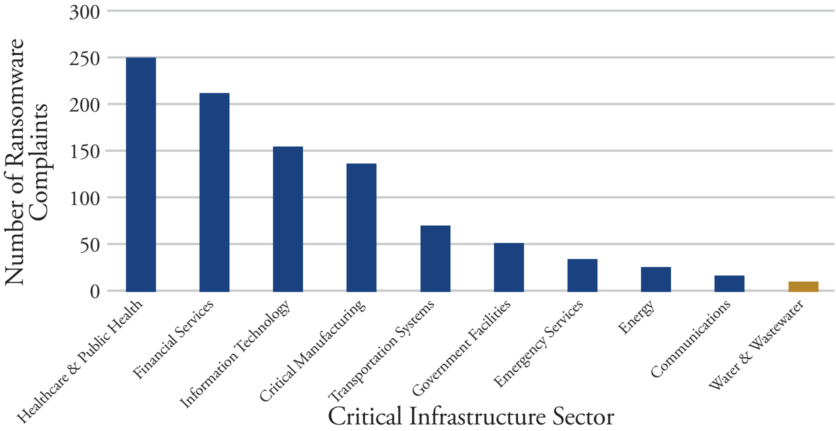
- **Aging SCADA & ICS Environments**
  - Many utilities run decades-old control systems with outdated firmware and no modern authentication or encryption, leaving them vulnerable to ransomware that could disrupt treatment and distribution processes.
- **Unvalidated Incident Response Procedures**
  - Few utilities conduct drills that simulate sector specific crises such as chemical dosing changes or pump outages, leaving readiness and coordination between IT and operations untested.
- **Minimal Sector-Specific Cyber Expertise**
  - Smaller utilities often lack staff trained in both water operations and cybersecurity, slowing detection of ransomware attacks and extending downtime during recovery.
- **Insecure OT-IT Links**
  - Administrative and operational networks are often interconnected, allowing ransomware to move from non-critical systems like billing into treatment plant controls.

WATER & WASTEWATER SYSTEMS SECTOR CYBERSECURITY

Action Checklist

- Develop and test a ransomware-specific Incident Response Plan for treatment, pumping, and distribution systems.
- Enforce Multi-Factor Authentication (MFA) on all remote access, SCADA interfaces, and administrative logins.
- Conduct annual tabletop exercises simulating chlorine feed changes, pump failures, and wastewater bypass events.
- Upgrade or segment legacy ICS and SCADA systems from IT networks
- Maintain offline, immutable backups of control system configurations, plant data, and administrative records.
- Assign a dedicated cybersecurity lead or train existing staff in both water operations and cybersecurity response.

Ransomware Complaints by CI Sector (FBI IC3 - 2024)



Notable Incidents

- **American Water Company (2024):** A ransomware shut down customer billing and service portals, including in Florida. Treatment and delivery continued, but customers faced delays in payments and service requests.
- **Veolia North America (2024):** A ransomware attack disabled billing and customer service systems for municipal water divisions, forcing a switch to manual operations. Restoration took weeks, delaying work orders and public service responses.
- **City of Oldsmar, Florida (2021):** Attackers gained remote access to a water treatment plant's SCADA system and attempted to raise sodium hydroxide levels. An operator detected the breach in real time and reversed the changes before the water supply was affected.
- **Baltimore Water System (2019):** A RobbinHood ransomware crippled billing and payment systems, leading the city to refuse ransom payment. Recovery efforts took months and cost over $18 million in restoration and cybersecurity upgrades.

Note: In 2023, the Water and Wastewater Systems sector reported only 8 ransomware complaints to the FBI, the lowest of any CI sector. While incident numbers appear small, legacy systems and limited detection capabilities mean the true risk is likely underreported.

State-Funded Resources & Education

Technical Tools

- **Florida Cyber Risk Assessment Ransomware Readiness**
  (https://cyberflorida.org/cip/)
- **FCC Communications Security, Reliability & Interoperability Council (CSRIC)**
  (https://www.fcc.gov/csric)

Templates & Planning

- **Cyber Florida Incident Response Plan Templates**
  Available Upon Request
- **NIST Cybersecurity Framework**
  (https://www.nist.gov/cyberframework)
- **FCC Cybersecurity Planning Guide**
  (https://www.fcc.gov/cyberplanner)

State-Funded Resources

- **FIU Cyber Leadership Courses**
  (https://gordoninstitute.fiu.edu/cybersecurity-policy/training/cybersecureflorida/index.html)
- **CISA Cyber Hygiene Services**
  Free Assessments & Scans
  (https://www.cisa.gov/resourcestools/ programs/cyberhygiene-services)