The OT Recovery Gap

10 Things Every Water Utility Should Know

Why recent cyber attacks on water and wastewater systems (WWS) organizations are really a recovery problem, and how PLC and device code backups get you back online in hours, not weeks.

ACT 1 The Threat

01 Water systems are being attacked at the PLC level — right now

30+ Minnesota communities | **12+ states**

In late July 2026, a coordinated campaign disrupted 30+ Minnesota communities and hit utilities in at least 12 states. The FBI and EPA issued a joint alert on July 30, 2026 after water and wastewater utilities in at least 7 states reported intrusions. Federal authorities describe a significant escalation in attacks on water-system devices.

02 Threat actors aren't just stealing data, they're rewriting your plant's logic

Loss of view | **Loss of control**

These intrusions didn't target customer records, they targeted the machines. According to the FBI/EPA alert, threat actors remotely accessed exposed PLCs, changed IP addresses and passwords to lock operators out, and modified project files and ladder logic, the actual program that runs pumps, valves, and treatment.

03 The physical consequences are severe

Pressure loss | **Flooding** | **Shutdowns** | **Boil-water advisories**

Reported impacts included loss of water pressure, flooding, temporary plant shutdowns, boil-water advisories, and the risk of untreated groundwater infiltrating pipes. In OT, a cyber incident isn't an inconvenience, but a public health event.

04 The vulnerability being exploited is not new and has no patch

CVE-2021-22681 | **CVSS 9.8** | **No vendor patch**

Much of the activity abused CVE-2021-22681 (CVSS 9.8), an authentication bypass in Rockwell Automation Logix controllers for which there is no vendor patch, along with internet-facing Allen-Bradley MicroLogix 1100/1400 devices. Only architectural defenses and a solid recovery plan stand between you and prolonged downtime.

ACT 2 Why Recovery Is the Real Problem

05 Getting hacked is fast. Recovering is not — that's the OT Recovery Gap

Detection has gotten fast; restoration hasn't. IT recovery means restoring data you almost certainly backed up. OT recovery means restoring the logic and configuration running physical equipment, often the one thing nobody backed up.

1 in 5

OT incidents still take over a month to fully recover, even though nearly half are detected within 24 hours

SANS 2025

06 Without a known-good version, teams rebuild controller code by hand

Days-to-weeks of manual reprogramming

When the PLC program has been tampered with and there's no clean known-good version, engineers reconstruct logic from memory, institutional knowledge, or outdated versions while the plant stays down.

07 Your IT backup plan does not cover the plant floor

Having a backup ≠ being able to restore

Standard backup tools capture servers and databases, not the code inside PLCs and industrial control systems. That code often lives only on the device itself or on a single technician's machine, with no versioned, offline copy anywhere. And the backups that do exist are frequently months old, untested, or online where the same threat actor can encrypt them. "We back things up" isn't the same as being able to restore that exact controller tonight.

08 Your backup itself might be compromised

Validate before you redeploy

Federal guidance now explicitly warns utilities to validate project-file backups before redeploying them because threat actors have shown they can plant malicious logic that ends up in the backup. Recovery isn't just having a version to roll back to; it's having a verified, known-good version you can trust.

ACT 3 The Solution & Payoff

09 Automated, versioned device code backups close the gap

Capture every device automatically | **Track every change** | **Restore the last verified version**

The fix is to back up device code the way software teams back up source code: automatically, versioned, and ready to restore. Capture PLC and industrial control system code across every device on a schedule instead of manual USB pulls, track each change so you can see exactly what a threat actor altered, and restore the last verified version on demand. Recovery shifts from days of manual reprogramming to a controlled restore, meeting the offline-backup and tested-restore practices the FBI/EPA and CISA now call for.

10 Recovery speed is a decision you make before the attack

~2 hrs

One Minnesota plant restored in about two hours

WITHOUT DEVICE CODE BACKUPS

Reconstruct programs by hand, uncertain what's clean, down for days or weeks.

WITH THEM

Pull the last known-good version, see exactly what changed, and return to service in hours.

In water and wastewater, uptime is public health, and the utilities that recover fastest already had their device code backed up, versioned, and ready to restore.