# Water Supply is a Data Center Risk


**Mark Trump**

Defense Advisor @ Capgemini | IT/OT Convergence, Critical Systems Defense

Two years ago, I wrote that our water supply was becoming a data center security problem. I'd rather have been wrong.

In April 2024, Dark Reading published my piece on liquid cooling, water dependency, and the security gap nobody owned. The argument was simple: water is a cyber dependency, not just a sustainability line item.

Since then:

- Aliquippa, PA (Nov 2023) — attackers disabled a PLC regulating water pressure, forcing manual fallback; a related incident at a small Irish utility left customers roughly two days without service.
- Arkansas City, KS (2024) - manual intervention prevented compromise of chemical dosing.
- Minnesota (July 2026) - coordinated attack hit more than 30 municipal water systems; Plymouth and South St. Paul reverted to manual operations and Maple Plain declared a local emergency. FBI/EPA reported utilities in at least seven states were affected, with pressure loss and flooding.

Meanwhile, the demand curve steepened: roughly two-thirds of 809 planned U.S. AI data center projects are sited in areas facing water shortages.

The good news is that every one of those incidents was survivable, because operators could still run manually. That's the lesson worth scaling.

Four moves that pay off now:
✓ Name water as a dependency in your risk register — with the serving utility identified by name.
✓ Get PLCs and HMIs off the public internet and kill default credentials.
✓ Rehearse manual fallback and a multi-day water-loss scenario in your crisis plan.
✓ Move new builds toward closed-loop/zero-water cooling and non-potable sources.