

NLC NATIONAL LEAGUE OF CITIES

RISC RISK INFORMATION SHARING CONSORTIUM

WHEN ONE ATTACK BECOMES THIRTY CLAIMS: WATER-SECTOR CYBER RISK & THE POOL'S ROLE

Jason Power

October 27 | 2:45 - 3:45 p.m.

When One Attack Becomes Thirty Claims

Water-sector cyber risk and a pool's role

PREPARED BY VC3 · SERVING LOCAL GOVERNMENT FOR 30+ YEARS

What we'll cover

A BRIEFING IN FOUR PARTS



01 · The risk, in your language

Why one coordinated attack is really a correlated, correlated, multi-claim aggregation event, not thirty separate member IT IT problems.



02 · How exposed the sector is

What the data actually says about how heavily water and public infrastructure are targeted, and why your book concentrates the risk.



03 · What "good" looks like looks like

The handful of low-cost practices that defeat the the vast majority of these these attacks, a benchmark benchmark for a healthy healthy member.



04 · Where the pool has has leverage

The levers only a league or pool holds to move member behavior at scale, and three questions to gauge any member's exposure.

PART 01

The risk, in your language

A well switched off is one story. Thirty of them in a weekend is a is a different one — an aggregation event.

One weekend. One actor. Dozens of members at once.

SECTION 1 · WHAT HAPPENED

Over the weekend of July 26, 2026, Iranian-affiliated hackers reached into the internet-connected control systems of dozens of U.S. water utilities by water utilities by changing administrator passwords, disrupting automated operations, and in at least one town, simply switching a well off. well off.

30+
water systems targeted in Minnesota

9
systems attacked in Michigan

7+
U.S. states with utilities hit

<1 wk
after federal advisory expanded

THE REFRAME

To a member, this is one IT incident. **To a pool, it is a single event that spawns claims across your book at the same moment:** the definition of a correlated, aggregated loss.

Why this is a pool problem, not a member IT problem

SECTION 1 · THE AGGREGATION LOGIC



Correlated, not independent

Members share the same handful of controller brands, brands, vendors, and remote-access habits. One
One exposed weakness is a template for hitting many many at once.



A severity line, not attrition

A single incident can trigger response, recovery, business-interruption and liability costs across multiple members in one window: concentrated, not spread out.



It reaches your reinsurance

Correlated losses are exactly what erode surplus and surplus and shape excess-of-loss renewals.
Aggregation is a portfolio question, not an IT ticket. ticket.

The unit of analysis isn't the well. It's your book and the shared weaknesses that let one attacker strike many members

PART 02

How exposed are members?

The honest data on how heavily water and public infrastructure are targeted, and why your members sit at the center of it.

Not the loudest sector but the most exposed

SECTION 2 · HOW HEAVILY TARGETED

70%

of all cyberattacks IBM X-Force responded to in 2024 were aimed at critical-infrastructure organizations.

~80%

year-over-year rise in ransomware against against the energy & utilities sector.

Named

repeatedly by GAO, EPA and CISA as one of one of the most vulnerable and attractive attractive targets in U.S. infrastructure.

Water is the sector federal authorities single out as the most exposed, and the pace of attacks on it is accelerating.

Sources: IBM X-Force Threat Intelligence Index (2024 data). Trustwave 2025 Energy & Utilities threat reporting. U.S. GAO (GAO-24-106744; GAO-26-109159), EPA and CISA advisories; U.S. Senate EPW testimony, Feb 2026.

Why water concentrates the risk in your book

SECTION 2 · THE STRUCTURAL DRIVERS

- **~150,000 public water systems** – most small, rural, and thinly staffed. The profile that fills a risk pool's membership.
- **Run by local governments** – so cybersecurity competes for funding with schools, roads and public safety, and usually loses.
- **Legacy operational technology** – control systems built decades ago for reliability, never for internet exposure.
- **70%+ failed basic standards** – of water systems inspected by the EPA since Sept 2023 fell short on fundamental cybersecurity.
- **Only ~1 in 5 use MFA** – multi-factor authentication, which blocks the overwhelming majority of account-takeover attempts, is still the exception and not the rule.

The exact profile attackers hit is the exact profile that fills a municipal pool's book.

Five years of the same open doors

SECTION 2 · THE PATTERN

2021

Oldsmar, FL

Attacker remotely raises lye in the water supply ~100x before an operator catches it.

2023

Aliquippa, PA

CyberAv3ngers hijack an internet-exposed controller; the the station drops to manual.

2024

American Water +

The largest U.S. water utility is is hit; Veolia's water division division suffers ransomware.

2025

Warnings intensify

CISA and EPA keep flagging a a sector failing the basics; exposed devices remain common.

2026

Coordinated campaign campaign

Dozens of utilities across 7+ states hit within days — same same weaknesses, at scale.

Scale and speed changed. The method, internet-exposed devices and default settings, has been the same, and flagged by federal advisories, for years. advisories, for years.

PART 03

What “good” looks like

None of these attacks were sophisticated. They walked through open through open doors, which means the risk is can be reduced.

The bad news is also the good news

SECTION 3 · THE TURN

None of these attacks required a nation-state exploit. They used open front doors, which means the fixes are known, affordable, and within reach for even a small member.



Internet-exposed devices

Controllers reachable directly from the public internet — no gateway, no barrier.



Default & shared passwords

Factory credentials like “1111,” or one password shared by everyone.



No multi-factor login

Remote access guarded by a single password an attacker can guess or reuse.



Little or no monitoring

No one watching the logs, so an intrusion goes unnoticed until something breaks.

Fix these four, and a member defeats the vast majority of everything we just walked through.

What “good” looks like for a member water system

SECTION 3 · THE BENCHMARK



OT off the open internet

Remote access routed through a controlled gateway — never a controller facing the public internet.



No default or shared passwords

Unique, strong credentials with a real password policy behind them.



MFA on remote & admin access access

Multi-factor required for any access from from outside the plant network.



IT / OT segmentation

Business and control networks separated so one breach can’t reach everything.



Logging — and someone watching

Centralized logs with a person or partner actually monitoring them.



Tested, offline backups

Controller logic and config backed up offline, and proven to restore cleanly.



A practiced response plan

A written incident-response and manual-operation plan that’s been rehearsed.



Knows who to call

Contacts for CISA, FBI and its device vendors ready before an incident.

The habits every district should run — always

These aren't water-specific. They're the baseline of modern security best practice — and they align with CISA's Cross-Sector Performance Goals. Performance Goals.

MFA everywhere

Phishing-resistant multi-factor on on every remote and admin login. login.

Patch & retire old gear

Keep systems updated; replace replace end-of-life equipment on a on a schedule.

Segment IT from OT

A DMZ and network segmentation between business and control systems.

Monitor & log

Centralized logging with someone (or a partner) actually watching it.

Least privilege

People and systems get only the access they truly need.

Tested backups

Regular, offline, and rehearsed so recovery is real, not theoretical.

Security awareness training

Staff who can spot phishing and social engineering.

A tested incident response plan

Written, assigned, and practiced before you need it.

Credible, free places to send a member

SECTION 3 · NO BUDGET REQUIRED

A pool doesn’t have to build any of this. Point members to resources that already exist, most of them free and federally backed.



CISA free services

No-cost vulnerability scanning and the Cross-Sector Performance Goals — a plain checklist any member can self-assess against.



EPA water-sector support

Water & wastewater cybersecurity assessments, guidance and technical assistance for utilities.



NRWA circuit riders

The National Rural Water Association’s cybersecurity circuit-rider program provides hands-on help to small and rural systems.



WaterISAC

Sector threat intelligence and alerts so a member hears about a campaign before it reaches them.

PART 04

Where the pool has leverage

You can’t patch a member’s controller, but you hold levers no levers no vendor and no member has.

The levers only a league or pool holds

SECTION 4 · YOUR INFLUENCE



The megaphone & the trust

You reach every member and you're a trusted, non-vendor voice. Awareness campaigns and briefings move behavior in ways a sales email never will.



Loss control & benchmarking benchmarking

Help members see where they stand stand against "what good looks like." like." A simple self-assessment turns turns an abstract threat into a to-do do list.



Incentives & grants

Premium credits, matching grants, or grants, or coverage conditions tied to tied to the basics are a way to pull an pull an entire membership toward toward MFA and off the open internet.



The coverage conversation

Underwriting questions and renewal touchpoints are natural moments to ask the few questions that most predict a member's exposure.

Three questions that reveal most of a member’s exposure

SECTION 4 · A TOOL TO TAKE WITH YOU

You don’t need a technical audit to gauge a member. Ask these three — the answers tell you most of what matters.

1

Is any control system reachable from the open internet, and if so, what stands in front of it?

Tests the single most common entry point in every case we reviewed.

2

Have you removed default and shared passwords, and turned on MFA for remote access?

Two cheap fixes that block the overwhelming majority of account takeovers.

3

If a controller went down tonight, could you run it manually and restore from a clean, offline backup?

Tests resilience and recovery — the difference between an incident and a crisis.

PARTNER WITH VC3

Let’s protect your members — — together

If you want to help your members get ahead of this, let’s talk. VC3 works with leagues with leagues and pools to educate members and deliver the services that turn “what turn “what good looks like” into reality, across your whole book, not one member at a member at a time.

- Credible, non-salesy education for your members
- Managed security services for members who want them
- Loss-control impact across your entire membership

Let’s start the conversation

Mark French Barrett

Director of Partnerships

mark.barrett@vc3.com

vc3.com



AIM HIGHER

Help your members close the open doors — before someone else walks through them.

Sources & further reading

FOR YOUR REFERENCE

- IBM X-Force Threat Intelligence Index — critical infrastructure share of incidents (2024 data; 2025 & 2026 editions).
- Trustwave — 2025 Energy & Utilities sector threat research (ransomware year-over-year increase).
- U.S. GAO — “Critical Infrastructure Protection: … Water and Wastewater” (GAO-24-106744, Aug 2024; GAO-26-109159, 2026).
- U.S. Senate Environment & Public Works — water-sector cybersecurity testimony (Feb 2026).
- Joint Cybersecurity Advisory AA26-097A — Iranian-affiliated actors exploiting PLCs (FBI, CISA, NSA, EPA, DOE, CNMF, Treasury; Apr 2026, expanded Jul 2026).
- CISA — Cross-Sector Cybersecurity Performance Goals; Joint-agency Secure Connectivity Principles for OT; free vulnerability-scanning services.
- EPA water-sector cybersecurity resources; NRWA cybersecurity circuit-rider program; WaterISAC.
- TIME, Axios, Smart Cities Dive & Cybersecurity Dive — reporting on the July 2026 multi-state water attacks.
- VC3 — “Cybersecurity Strategies for Water Systems” guide (MFA adoption and inspection-failure figures).