THE FULCRUM GROUP
One Technology Solution: Yours

The Cybersecurity Crisis

What Water District Leaders Need to Know NOW

Published by The Fulcrum Group, Inc.
February 2026

The Water District Cybersecurity Crisis

NEW And Critical Protections every Water District or City MUST HAVE IN PLACE NOW: For IT-to-OT Attacks, Vendor Access Risk, and the Controls That Prevent Disruption.

Built for Texas water and wastewater entities managing lean teams, distributed sites, vendor access, and OT/SCADA environments—where downtime isn't just expensive, it's operational.

"WWSs are frequent targets of malicious cyber activity, which has the potential to interfere with operations and may result in significant response and recovery costs. Of particular concern, a cyberattack on a vulnerable WWS may allow an adversary to manipulate operational technology (OT), which could disrupt the production of clean and safe water."-

EPA Guidance on Improving Cybersecurity at Drinking Water and Wastewater Systems- Revised August 2024

Provided as an educational service by: The Fulcrum Group, Inc.

Author: Steve Meek, CISSP

Phone: 817-337-0300 Email: steve@fulcrumgroup.net Web: www.fulcrumgroup.net

NOTICE: This guide is written in plain language for water and wastewater district leaders and operators. It is not legal, regulatory, or cyber insurance advice. Every water system and organization is different.

Use this as a leadership playbook — and involve qualified experts for decisions that affect safety, compliance, and emergency response.

About The Author

Steve "The Doctor" Meek, CISSP, is a 30+ year IT and cybersecurity veteran, CEO of The Fulcrum Group in Keller, Texas, and has been nationally recognized in his community. Won the inaugural 2024 MSP Titan of Industry Award winner for Community Impact for his service locally and to the IT community. Additionally, his firm has been recognized as one of the top 500 managed service providers in the US, via back-to-back national recognition on the **MSP 501 and CRN Top 500** — the IT industry's equivalent of making the honor roll at two different schools, except with more Office 365 tenants and fewer gold stars.

The Fulcrum Group has spent 24+ years serving Texas cities, local governments, water districts, healthcare organizations, and manufacturers — not from a call center in another state, but from a 100% Texas-based team that actually answers the phone. He holds a BBA from Angelo State University and has held multiple technical certifications from vendors such as Microsoft, Cisco, VMware and organizations such as ISC2 and CompTIA.

Steve's nickname isn't a marketing gimmick. It comes from something simpler: the belief that good technology leadership, like good medicine, is about ***listening and gathering fact-based metrics, before prescribing a solution.*** He now also hosts the business leader **Talk To Th3 Doc** podcast and has spent decades helping CEOs, city managers, and district leaders make technology decisions with clarity and confidence — not fear.

CREDENTIAL	EXPERIENCE	AWARD	RECOGNITION
CISSP Certified	**30+ Years in IT**	**2024 MSP Titan of Industry**	**MSP 501 & CRN Top 500**

Channel Futures. Leading Channel Partners Forward
MSP 501
2024 WINNER

THE CHANNEL CO.
CRN
MSP 500
2025

Why Water Districts Are a Prime Target Right Now

Threat actors — from ransomware groups to nation-state hackers — specifically target water and wastewater systems. This isn't paranoia. Federal agencies have issued repeated warnings backed by documented attacks. Here's some water districts industry and general metrics that help shape the dangers:

70%	26.6m	88%	30%
of water systems inspected by EPA fail "basic" cybersecurity	People affected by EPA 2024 report critical or high vulnerabilities	Of breaches that involve stolen credentials	Incidents that involve third-parties

Water district challenges that make cybersecurity difficult and high impact:

- Systems that must stay running 24/7 — downtime isn't an inconvenience, it's a public health emergency
- Distributed assets — treatment plants, pump stations, lift stations, storage tanks — spread across wide service areas with multiple entry points
- Heavy vendor dependence for telemetry, SCADA platforms, radio communications, and maintenance support
- A mix of legacy OT equipment and modern IT systems that can't always be patched like a standard office PC
- Public accountability that makes any operational disruption visible, politically damaging, and very difficult to quietly manage

EPA WARNING: Nation-State and Criminal Actors Are Already Inside the Sector

A series of documented attacks includes Russian hacktivists linked to Sandworm targeting multiple Texas water systems — including one in Muleshoe that caused an overflow — and Iranian-linked group Cyb3r Avengers compromising programmable logic controllers at a Pennsylvania water authority. GAO confirmed that nations, cybercriminals, and others have already targeted the nearly 170,000 U.S. water systems, which are increasingly automated.

💧 *Think your district is too small to matter? Attackers are money-focused and so easier targets are more likely a pay day. They actively prefer the smaller systems because they assume fewer defenses, smaller security budgets, and a higher chance you'll just pay the ransom to get the water flowing again. Flattering? Not exactly.*

IT vs. OT: The Difference That Makes or Breaks Your Response

Most water districts operate in two technology worlds. External support organizations may not always understand the relationships and different needs.

IT — Information Technology	OT — Operational Technology
Email, billing, HR, finance, file storage, phones, Microsoft 365 — your everyday office world. If it breaks, someone opens a ticket and complains.	SCADA, HMIs, PLCs, RTUs, and industrial control systems — the hardware and software that moves water. If this breaks, your community notices long before any ticket gets opened.

THE CRITICAL INSIGHT: Most cyber incidents start in IT — because email and user credentials are easy targets. Attackers then pivot or attempt to move laterally toward OT, where disruption creates maximum leverage. That pivot is exactly what you must prevent. Think of IT as the front door and OT as the boiler room. One unlocked desk in the lobby shouldn't mean a stranger can adjust your chemical dosing systems.

The term 'air-gapped' has become the 'I exercise regularly' of water district cybersecurity. Everyone says it but not everyone means it, or exactly understands it. The normal use of laptops, USB drives, vendor support sessions, and temporary connections have a remarkable talent for bridging gaps that were supposed to stay air-filled.

The 6 Biggest Cybersecurity Challenges for Water Districts

These aren't hypothetical scenarios. They are the patterns The Fulcrum Group's team sees periodically when working with Texas local governments and water systems — and they align directly with what EPA and CISA flags as priority risks to improve your security posture.

1. Remote Access Sprawl (Especially Vendor Access)

Vendor access is one of the fastest-growing attack surfaces in the water sector. When every integrator has their own VPN tunnel, every vendor uses a different access method, and nobody tracks when sessions are active, oversight becomes nearly impossible. A centralized, DMZ-brokered remote access model — with consistent authentication, logging, and session monitoring — is the right standard. Additionally, firewall-based VPNs frequently require updates and it zero trust tools to replace should be considered.

If you've ever said 'the SCADA vendor said he'd log on later, without you turning on the access,— congratulations, you've just probably described an unlocked back door that nobody is watching.

2. Internet Exposure You Didn't Know You Had

OT devices like PLCs, RTUs, and HMIs are easy targets when exposed to the public internet — and many districts have exposure they've never mapped. CISA regularly releases Advisories detailing vulnerabilities and possible updates to firmware or other mitigations.

Cyber hygiene scanning programs regularly surface assets that no one realized were accessible from outside the district's network. Attackers scan the public Internet and are looking for low-hanging fruit. Automated pentesting can add enhance the effort for more qualified scanning intelligence, to both inside and outside your network.

3. Legacy OT That Can't Be Patched Like IT

Obsolete controllers and aging field devices present a known and growing risk. Because operational schedules make immediate replacement impractical, compensating controls become critical: network segmentation, hardened jump hosts, protocol gateways, strict access restrictions, and detailed logging to fill the gap until equipment can be replaced.

> ⏳ *That 15-year-old PLC running your pump station isn't charming — it's a vulnerability with a blinking cursor. Replacing it takes time and budget. But protecting it in the meantime takes planning, not magic.*

4. Flat Networks That Enable Lateral Movement

When IT and OT environments share the same flat network without segmentation, an attacker who compromises an office workstation can move directly toward operational systems.

5. Visibility Without Verification

Many districts have monitoring tools installed but don't consistently review logs, alarms, remote access sessions, or account activity. That's like installing cameras at your pump station but never checking the footage — even after an alarm triggers.

> 🤖 *AI might even be able to help with review, but make sure to lock down your AI so logging information doesn't get out.*

6. People and Process Gaps

Small teams with heavy workloads are the norm in public water. Cybersecurity can't run on heroics alone. It needs repeatable processes, documented roles, and clear escalation paths established long before a crisis starts. Time may not be on our side, with elder experts retiring and dependence on tribal knowledge could leave facilities at a higher risk.

“But We’re Small — Who Would Target Us?”

This is the most common question we hear — and the most dangerous assumption in the water sector.

Threat actors specifically target small and mid-sized water systems because they assume:

- Fewer security controls are in place
- Little or no dedicated IT
- Limited cybersecurity staff or capabilities
- A higher likelihood of paying a ransom or accepting disruption to restore service quickly

🎯 *The ‘we’re too small to matter’ theory works great until the moment it doesn’t. Ransomware doesn’t check your annual budget before it encrypts your SCADA historian. It just checks whether the door was unlocked.*

Water and wastewater systems are frequent targets of malicious cyber activity. These threats are active and ongoing — and federal agencies like the EPA and CISA have issued specific guidance because documented attacks have already hit systems just like yours.

THE GOOD NEWS: The best defense doesn’t require a massive budget. It requires a focused set of high-impact controls applied consistently. That’s exactly what The Fulcrum Group’s STARPower™ Framework is designed to deliver — practical security outcomes without requiring you to hire an army of consultants.

Your 90-Day Cybersecurity Action Plan

If your team did only these six things in the next 90 days, you would be meaningfully safer — and better positioned for EPA compliance reviews, cyber insurance renewals, and board-level reporting.

01	02	03	04	05	06
Exposure Map	Vendor Access	OT Asset Inventory	Segmentation	Backup Recovery	Tabletop Exercise

🔍 1

Map and Reduce Internet Exposure

Identify every asset accessible from outside your network, especially anything OT-related. Remove what isn’t required. This is your single highest-priority action — everything else builds on knowing what’s exposed.

- ✓ Catalog all public IPs, private IPs, device names, and associated required ports

✓	Flag every OT-related asset with external visibility — HMIs, RTUs, historian portals, vendor gateways
✓	Remove or firewall any exposure that has no documented operational justification
✓	Treat every 'temporary' exposure as permanent until you prove otherwise

2 Inventory and Standardize Vendor Access

Document every vendor remote access method currently in use. Scattered access paths are one of the most exploited gaps in the water sector. Begin consolidating toward a centralized, controlled model.

✓	List every vendor, integrator, and contractor with any form of remote access
✓	Document the method: VPN, RDP, TeamViewer, AnyDesk, permanent tunnel, or shared account
✓	Consolidate toward a DMZ-brokered approach with logging and session management
✓	Implement just-in-time (JIT) activation — connections on when needed, off when not

3 Build Your OT Asset Inventory

You cannot protect what you haven't found. Focus first on internet-connected devices and any system that cannot be operated manually if it goes offline.

✓	Identify all PLCs, RTUs, HMIs, historians, and engineering workstations
✓	Map radio links, cellular connections, and wireless access points in the field
✓	Note every device that has no manual override — these are your highest-priority assets
✓	Cross-reference against your vendor access list to confirm every device has a known owner

4 Validate Segmentation and Tighten Zone-to-Zone Traffic

Confirm that IT and OT are properly separated. A flat network is an attacker's best friend — one compromised office laptop should never become a path to your SCADA systems.

✓	Verify a real boundary exists between IT and OT — not just a policy, but a technical control
✓	Apply 'deny by default' policies between all network zones
✓	Close every path that has no documented operational justification
✓	Confirm your DMZ is isolating external-facing systems from core OT

Test OT/SCADA Backup and Recovery

5

Backup files nobody has tested are just hope stored on a drive. Verify that your critical OT systems can actually be restored — and document every step while you do it.

✓	Confirm configuration backups exist for all PLCs, RTUs, and network devices
✓	Test restoration of HMI project files, historian databases, and alarm configurations
✓	Document the full restoration process, timing, and who executes each step
✓	Store backup credentials securely and separately from the systems they protect

🎯 **6**

Run a Tabletop Exercise

A plan that has never been tested is just a document. Simulate a cyber incident that includes SCADA disruption and vendor coordination. Find the gaps before a real attacker does.

✓	Scenario: ransomware locks your IT network and begins moving toward OT
✓	Who decides to isolate OT segments — and how fast can they do it?
✓	How do you coordinate with SCADA vendors during an active incident?
✓	What's your communication plan with your board, customers, and regulators?

Ready to Take the Next Step?

Knowing where to start is often the hardest part. The Fulcrum Group works with Texas local government entities, water and wastewater districts to cut through the complexity and focus on what matters most: protecting the systems that keep your community safe.

Contracts

The Fulcrum Group holds several contracts that can help organizations do business with us in the state of Texas.

- **DIR Contract # DIR-CPO-TMP-570** focuses is on providing managed IT solutions and related services under the Texas Department of Information Resources Cooperative Contracts Program.
- **NCTCOG Contract # 2025-018** is a master services agreement on TXShare where we agree to provide artificial intelligence solutions for public sector entities under the North Central Texas Council of Governments program.

We bring 30+ years of IT and cybersecurity experience, a 100% Texas-based team, and a "No IT Jerks" philosophy that means you'll actually enjoy working with us. (We know. Rare. We're proud of it.)

Schedule Your FREE Water District Cyber Readiness Conversation

A confidential, no-pressure session with our consulting team focused on SCADA and critical infrastructure.

☑ Pinpoint your top exposure risks ☑ Build your 90-day priority list

☑ Turn cyber-speak into clear decisions

No drama. No scare tactics. No judgment. Just a real conversation with people who have seen it all and fixed most of it.

Call: 817-337-0300

Email: sales@fulcrumgroup.net

Visit: https://www.fulcrumgroup.net/it-services-for-texas-water-and-wastewater-districts/

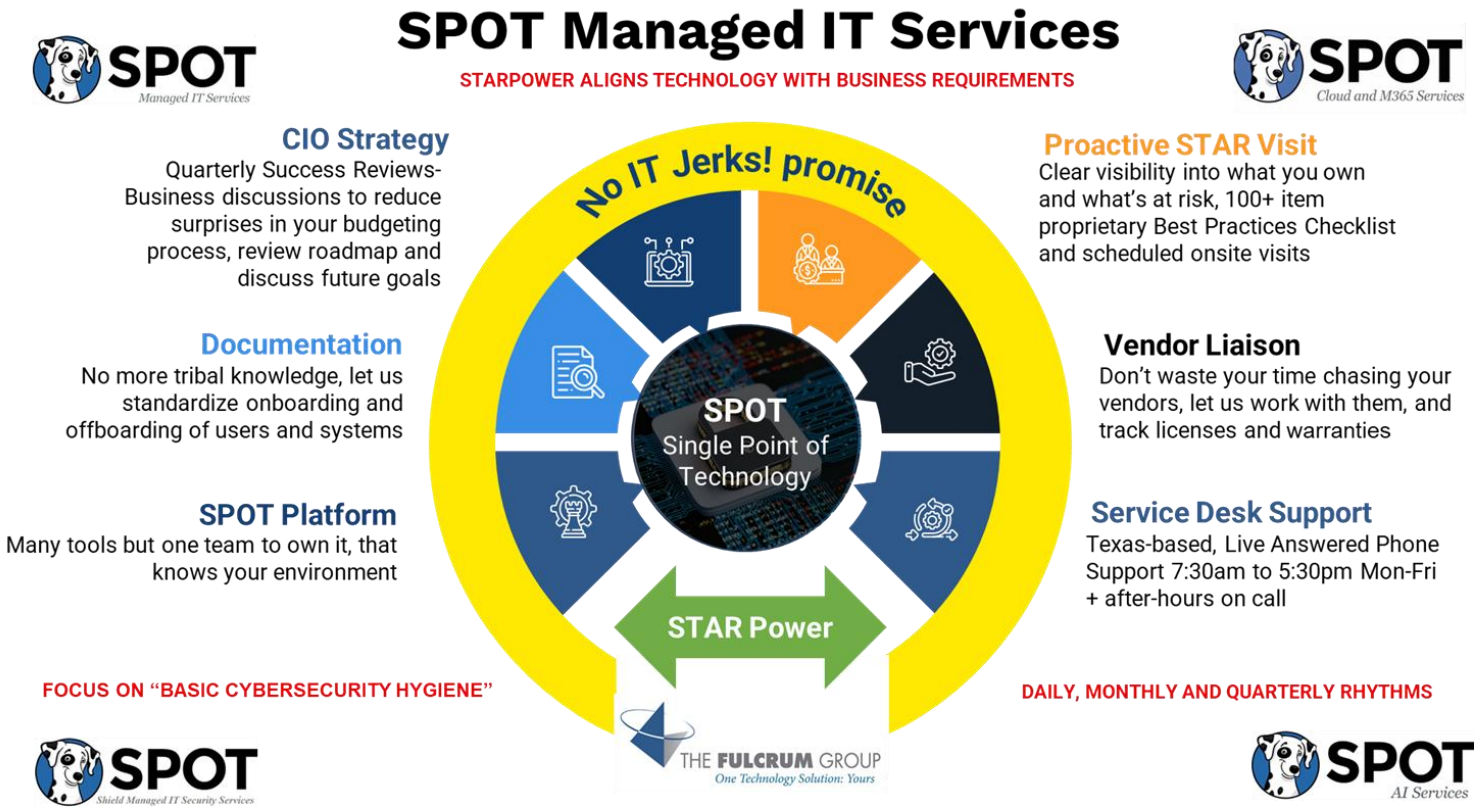
About The Fulcrum Group, Inc.

Founded in Keller, Texas in 2001, The Fulcrum Group is a 100% Texas-based managed IT and cybersecurity firm with 24+ years of experience serving local governments, water and wastewater districts, healthcare organizations, and small-to-mid-sized businesses across the DFW region.

Recognized in the IT industry nationally and locally, Fulcrum brings enterprise-grade security thinking to organizations that can't afford enterprise-level complexity. The firm holds a Texas DIR Contract (# DIR-CPO-TMP-570) and a NCTCOG/TXShare Contract (# 2025-018), making it straightforward for Texas public sector entities to do business without lengthy procurement battles.

Fulcrum's flagship SPOT Managed IT Services and SPOT Managed Security Services platforms — powered by the proprietary STARPower™ Framework — give water districts a structured, repeatable path to stronger security, modernized operations, and technology planning that actually makes sense for lean public-sector teams.

No offshore call centers, no cookie-cutter playbooks and especially No IT jerks. Just a local team that picks up the phone, knows your environment, and stays until the problem is solved. If you manage critical infrastructure and you're tired of feeling like a number on a service ticket, The Fulcrum Group was built for exactly that conversation.



Final Word From The Doctor

You don't need perfection. You need clarity and a place to start.

If your SCADA remote access is unmanaged, if vendor pathways are scattered, or if OT segmentation is more of a concept than a reality — that's exactly where we begin. When something goes sideways, and the data says it's a matter of 'when' not 'if,' you'll be glad you built a buffer between a threat actor and the systems that keep water safe for your community.

We built Fulcrum with one core belief: you deserve an IT partner who speaks plain English, shows up like a teammate, and never makes you feel dumb for asking questions. That's the "No IT Jerks" promise — and it extends to every water district conversation we have. If you need help with the day-to-day management of your technology, and some expertise in cybersecurity, we are probably a good match.

We're here when you're ready. The water can't wait.

— Steve "The Doctor" Meek, CISSP
CEO, The Fulcrum Group, Inc. • Keller, Texas