BOARD BRIEFING SUMMARY

Water District Cybersecurity: What Your Board Needs to Know

A one-page summary for district leadership and board members

Steve "The Doctor" Meek
CISSP • CEO, Fulcrum Group
817-337-0300

70%+	26.6M	$43.5B
of water systems fail basic EPA cyber standards	Americans served by systems with critical vulnerabilities	at risk from a single day of water service disruption
EPA Enforcement Alert, 2024	*EPA OIG Report, Nov 2024*	*U.S. Water Alliance*

THE RISK: WHY YOUR DISTRICT IS A TARGET

🎯	**You Must Stay Running**	Water systems cannot afford downtime. Attackers know this — it's exactly why they target utilities with ransomware.
🔗	**Vendor Access Gaps**	Every integrator with an unmonitored connection is a potential entry point. Most districts have several.
udea8	**Nation-State Threats**	Russian and Iranian actors have already attacked Texas water systems. This is documented, not theoretical.
⚠️	**Legacy OT Equipment**	Old PLCs and RTUs can't be patched like office PCs. They need compensating controls until replaced.
📧	**Phishing + Credentials**	88% of breaches involve stolen credentials. One compromised employee account can start the chain.

5 QUESTIONS EVERY BOARD MEMBER SHOULD BE ABLE TO ANSWER

1	What are our top 10 'must-not-fail' systems, and who is responsible for each?
2	Do we have MFA enforced for all users — especially anyone with admin access or vendor credentials?
3	When did we last test a restore of our SCADA or OT system backups?
4	Who decides to isolate our OT network during a cyber incident — and how fast can they do it?
5	Have we mapped every vendor with remote access to our systems and confirmed those paths are monitored?

THE 6 ACTIONS YOUR TEAM SHOULD COMPLETE IN THE NEXT 90 DAYS

#	Action	Target Window
1	Map and reduce internet exposure — especially OT-facing assets	**Days 1–15**
2	Inventory and standardize all vendor remote access methods	**Days 1–15**
3	Build your OT asset inventory starting with internet-connected devices	**Days 16–45**

4	Validate IT/OT segmentation and apply ‘deny by default’ zone policies	Days 16–45
5	Test OT/SCADA backup restoration and document the process	Days 46–90
6	Run a tabletop exercise simulating SCADA disruption + vendor coordination	Days 46–90

Want to bring this to your board with confidence?

The Fulcrum Group offers a FREE, confidential Water District Cyber Readiness Conversation. We’ll work through these six actions with you, identify your highest-risk gaps, and give you a clear starting point — no pressure, no jargon, no IT jerks.

817-337-0300
fulcrumgroup.net
fulcrumgroup.net/water-cyber
Keller, TX • 100% Texas-Based Team