A prescriptive approach to securing your water utility in a hurry.

The recent attack on Oldsmar, in which a hacker routed through a remote access system designed for IT troubleshooting in an attempt to poison the town's water supply, has highlighted a need for increased cybersecurity measures in the water industry.

Following the Oldsmar breach, there are three ways your team can respond:

1 Align with baseline cybersecurity standards for industrial controls (IEC 62443 or NIST 800-82 and its supporting special publications).

Replace your remote access system with one that includes, at a minimum:

- A Moving Target Defense SD-WAN.
- A standardized, form-based access control system.
- Session recording.
- Off-premises single-use virtual desktops.
- Multi-factor authentication.
- User-session-protocol specific whitelisted access to equipment.
- 4-eye consent capability.
- Backup communications circuits.

And, ideally,

- Defines a clean break between operational networked equipment and IT systems.
- Includes behavioral analytics and monitoring, so you know if the person using the terminal changes or starts to do something unexpected.
- Deploys password managers for the personal and professional use of your employees.
- Takes under 30 seconds to connect through.

After you've deployed the remote access system, walk the floor scanning for, and removing, unauthorized cellular connections.

2 "Starting today, no one gets in here without looking me in the eye."

- Disconnect your plant equipment from the Internet.
- Walk the plant floor scanning for, and removing, cellular connections.

3 "Let's hold off on making any changes."

Doing nothing is always a choice. Respectfully, in this situation, it is a bad one.

How much should Option 1 cost?

Were you to use Dispel, the above would likely cost between $25-50k per year, require you to plug one box into your system, and, after taking staff training into account, would likely take 2 days to roll out.

If you would like to see this system in action, contact us at enterprise@dispel.io or visit us at https://www.dispel.io.

For utilities that want to keep operations running but need more time to deliberate: Dispel is providing free 3-month deployments followed by 50% off for the rest of 2021.

If you would like an alternative single-source provider to Dispel, we highly recommend Dexter Edward. We do not know how much a deployment of theirs would cost, but they are good people, and their engineering is phenomenal. You can reach them at info@dexteredward.com or by going to https://www.dexteredward.com.

I run a water utility, what should I read?

The most accessible documents on cybersecurity for operational technology settings are the National Institute of Standards and Technology's (NIST) Special Publications. Our advice is to skip the breathless consultant presentations and instead make a very large pot of coffee and read NIST 800-82 (Guide to Industrial Control Systems (ICS) Security (nist.gov)) and NIST 800-160 volume 2 (Developing Cyber Resilient Systems: A Systems Security Engineering Approach (nist.gov)).

If you want to know how to manage cybersecurity across both industrial systems and informational technology, we recommend also reading the NIST Cybersecurity Framework ("the NIST CSF"), which you can download here: (Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1 (nist.gov)).