ARCHITECTING RESILIENCE

How to Keep Wastewater Running When Ransomware Strikes

The call came on a Tuesday morning. A mid-sized American city had been hit by ransomware. Email systems were down. Business applications were frozen. Servers were encrypted. IT teams scrambled to assess the damage as the full scope of the attack became clear. But in the midst of this chaos, something remarkable happened: the city's wastewater treatment systems continued operating normally. The pumps kept running. The SCADA systems remained secure. The critical infrastructure that residents depended on for public health and safety never faltered.

A NEW ERA OF INFRASTRUCTURE THREATS

We're living through a fundamental shift in how nation-states and criminal organizations target critical infrastructure. The scope and sophistication of these threats became starkly clear in late 2023 when the FBI discovered that China had infiltrated approximately 200 U.S. water utilities—some with access dating back at least five years. Among them was Littleton, Massachusetts, a town of just 10,000 residents whose water utility manager asked the FBI a question none could answer: "Can you think of any reason that China would target us?" (CBS, 2025).

The answer, according to General Timothy Haugh, who led both the National Security Agency and U.S. Cyber Command until his dismissal in April 2025, is chilling: "There is no other reason to target those systems. There's no advantage to be made economically. There was no foreign intelligence collection value. The only value would be for use in a crisis or a conflict."

But China isn't the only threat. The group known as CyberAv3ngers has emerged as Iran's most active hackers focused on industrial control systems.

Over the past 18 months, CyberAv3ngers have disrupted more than 100 control devices globally, highlighting how geopolitical groups are now probing industrial systems as strategic leverage. They didn't just vandalize systems—they rewrote the "ladder logic" code that governs device functionality, actually disrupting service at multiple locations.

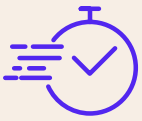
If anything, it's intensifying as water treatment systems become increasingly digitized and interconnected. The strategic calculation is clear: by threatening to disrupt water, power, and other essential services, adversaries hope to keep American resources focused at home rather than abroad, or to deter U.S. intervention in a conflict altogether.

WHY WASTEWATER INFRASTRUCTURE IS A PRIME TARGET

The U.S. water treatment market is projected to reach $42.3 billion by 2030, driven by rapid industrialization, aging infrastructure, and tightening environmental standards (IndustryARC, 2024). As facilities modernize with advanced filtration technologies, IoT sensors, and AI-powered monitoring systems, they're also expanding their digital attack surface.

Wastewater treatment facilities present an especially attractive target for several reasons:

Critical to public health.
Disrupting wastewater treatment can have immediate health consequences for entire communities. The threat alone creates leverage for attackers seeking to cause panic or extract ransom payments. As one Senate cybersecurity leader noted, if China took just three or four utilities offline simultaneously, "the entire country would be focused on it," achieving exactly the distraction adversaries seek.



Outdated security practices and resource constraints.
Many water and wastewater systems were built decades ago, then retrofitted with remote monitoring and control. Tight budgets and limited cybersecurity expertise often leave vulnerabilities unpatched or equipment unsupported—creating easy entry points for attackers.

Convergence of IT and OT.
As operational technology converges with information technology, facilities create pathways for attackers to move from less-secure business systems into the industrial control systems that actually operate the treatment processes. Once inside, sophisticated adversaries don't always install obvious malware. Instead, they steal login credentials and masquerade as legitimate employees, making detection far more difficult.

WHEN PREVENTION ISN'T ENOUGH: THE OHIO CITY CASE STUDY

The city I mentioned at the beginning of this article took a different approach to securing their wastewater infrastructure. Rather than assuming they could prevent every attack on their general network, they built their operational technology architecture with the assumption that their IT systems would eventually be compromised.

They deployed secure remote access technology throughout their wastewater plant—across PLC panels, control room devices, and remote pump stations. Each site connected through cellular private networks with multiple layers of segmentation separating the operational technology from the city's general business network.

When ransomware spread through city servers, wastewater systems remained online, requiring only access key resets once IT was restored.

This outcome wasn't accidental. It was the result of several key architectural decisions:

- **Network segmentation.** The operational technology network was completely separated from the IT network, with no direct pathways between them.
- **Secure remote access.** Rather than using VPNs that bridge networks together, the facility used a solution that creates secure tunnels between specific devices without ever exposing the OT network.
- **Cellular redundancy.** Remote sites used cellular connections, ensuring that even if the primary network was compromised, operations could continue through alternative pathways.
- **Minimal attack surface.** The secure access solution presented almost no attack surface to the internet, making it nearly impossible for ransomware or other malware to propagate into the OT environment.

The contrast was stark: while the city's IT staff spent weeks rebuilding systems and restoring data, the wastewater operations continued without interruption. No treatment processes were affected. No public health risks emerged. The facility maintained compliance with all environmental regulations.

BUILDING RESILIENCE WHEN YOU CAN'T ELIMINATE RISK

1 ASSUME BREACH, DESIGN FOR CONTAINMENT

Design your architecture assuming your IT systems will be compromised. Eliminate direct pathways between IT and OT networks. Use secure remote access or cellular redundancy to connect only where necessary, and maintain true air gaps for critical systems.

2 IMPLEMENT DEFENSE IN DEPTH

Multiple layers of security mean that if one control fails, others remain in place. This includes network segmentation, secure remote access, application whitelisting on OT systems, and continuous monitoring for anomalous behavior.

3 PLAN FOR BUSINESS CONTINUITY

Document how operations can continue even if your primary access methods are compromised. Ensure cellular or other out-of-band connectivity options exist. Test these failover mechanisms regularly.

4 INVEST IN DETECTION AND RESPONSE

You need visibility into what's happening on your OT network. Deploy monitoring solutions designed specifically for industrial control systems. Establish baselines for normal behavior to quickly identify anomalies. Remember that sophisticated attackers may not install obvious malware but steal credentials to masquerade as legitimate users.

5 CONDUCT REGULAR ASSESSMENTS

Organizations like the Ohio Cyber Reserve offer free cybersecurity audits for critical infrastructure. These assessments provide valuable outside perspective on vulnerabilities you might not see from inside your organization.

6 TRAIN YOUR TEAM

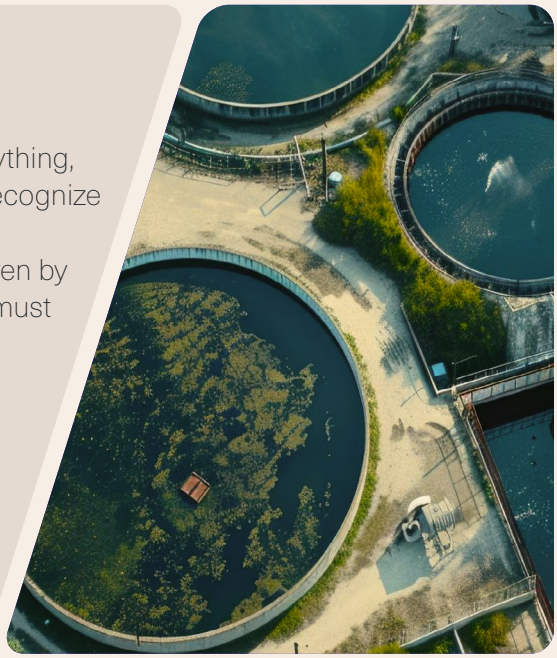
Your operators need to understand the cybersecurity implications of their actions.Many breaches begin with social engineering attacks on staff who have access to critical systems.

THE PATH FORWARD

The threats facing wastewater infrastructure aren't going away. If anything, they're accelerating as geopolitical tensions rise and nation-states recognize the strategic value of pre-positioning capabilities in American critical infrastructure. The market for water treatment is growing rapidly, driven by environmental regulations and aging infrastructure, but this growth must be accompanied by equally robust investment in cybersecurity.

The Ohio example proves resilience is possible when OT is isolated and secured. The question isn't whether to invest - it's whether you can afford not to.

The only question is whether you'll be ready when they press that red button.



Sakari Suhonen, CEO of Tosi US, is a proven leader in OT cybersecurity and network automation. With over 20 years leading B2B software companies, he has transformed organizations and driven exceptional growth, including spearheading Finland's first B2B enterprise SaaS company IPO. His business acumen and innovative approach have established him as a respected executive with a consistent track record of delivering results.

Sakari Suhonen
CEO, Tosi US
(formerly Tosibox US)

US HQ
1212 Corporate Drive
Suite 170
Irving, Texas 75038

GLOBAL HQ
Elektroniikkatie 2a
7th floor
90590 Oulu, Finland

CONTACT US

in tosi