CISO GLOBAL

A **CISO GLOBAL** WHITE PAPER

WATER SECTOR:

Tackling IT Security Fundamentals

Table of Contents

For more information, please contact us
480-389-3444 or visit **www.ciso.inc**

Water Sector Modernization and Digital Transformation

Water and wastewater facilities are facing a crucial time in their journey to modernization, as Digital Transformation is bringing about a shift in risk. Next gen technology can transform your water operations, but some fear introducing cyber. For those of us who specialize in cybersecurity and critical infrastructure, it was no surprise that cybersecurity has become one of the top concerns facing the water sector[1]. As industry modernization projects like smart water systems and advanced data analytics are rolled out, we can only expect this trend to rise, with cybersecurity at center stage as the number one concern. Cybersecurity is a growing concern not just within the water sector, but across all industries. In fact, in the first quarter of 2023, the US Cybersecurity and Infrastructure Security Agency (CISA) updated its Cross-Sector Cybersecurity Performance Goals (CPGs) to help lay the foundation for fundamental cybersecurity practices for critical infrastructure.[2] Solving an issue of this magnitude is going to take a community and partnership approach to help water facilities create a culture of cybersecurity that includes addressing fundamentals, assessing risks, openly sharing threat intelligence, managing vulnerabilities, monitoring networks, and securing supply chains.

Is There a Shortcut?

Building a successful cybersecurity program takes real effort and commitment. Long gone are the days that an effective cybersecurity defense was a basic firewall, anti-virus software installed on a few workstations, and an outdated security policy sitting in a drawer. Today's threat

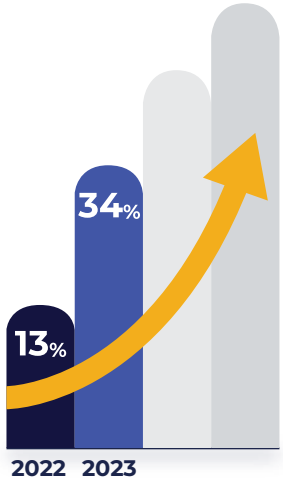
> "[Only] **31% of utilities** plan to update existing **IT systems** to **guard against** intrusion."
>
> – AWWA, 2023

landscape is riddled with advanced attackers who are backed by hostile nation-states and deliver business-crippling ransomware that costs millions to clean-up. Despite the obvious dangers of infection, third-party vendors often connect laptops or removable storage devices directly into networks without prior cybersecurity checks, and 84% of industrial sites have at least one device that is remotely accessible.[3] That is a shockingly low number,

but is – again – unsurprising. This metric reflects the realities of building and maintaining an effective security program. Few utilities (or larger, established companies for that matter) have the budget and resources to fully implement a security program by themselves. Building strategic partnerships with security-first vendors and the wider community are essential to fully develop a security strategy. How effectively water facilities identify the right partners decides whether they delay or accelerate their IT security goals and plans. Experienced partners will help conserve budget, streamline efforts, and maximize ROI. At CISO Global, one of our mottos is *Security Is a Team Sport*. Tackling the challenges of cybersecurity will require a whole team of industry peers, partners with expertise, and the wider IT and cybersecurity communities.

The Fundamentals

The number of unpatched security vulnerabilities is significantly increasing. In fact, a 2023 report from AWWA found that 34% of security vulnerabilities impacting industrial control centers remain unpatched, compared with 13% the previous year.[4] In 2019, the WaterISAC (the international security sharing network created by and for the water & wastewater sector) published updated cybersecurity guidance that outlines 15 fundamental security controls to help guide utilities and organizations in developing a security program. (It should be noted that these controls are not ranked by priority, and all organizations should consider each control as a vital component of their overall strategy.)



Unpatched security vulnerabilities impacting ICSs are **significantly increasing, 34% in 2023, vs 13% the previous year.**

(The Hacker News, 2023)

1. Perform Asset Inventories
2. Assess Risks
3. Minimize Control System Exposure
4. Enforce User Access Controls
5. Safeguard from Unauthorized Physical Access
6. Install Independent Cyber Physical Safety Systems
7. Embrace Vulnerability Management
8. Create a Cybersecurity Culture
9. Develop and Enforce Cybersecurity Policies and Procedures
10. Implement Threat Detection and Monitoring
11. Plan for Incidents, Emergencies, and Disasters
12. Tackle Insider Threats
13. Secure the Supply Chain
14. Address All Smart Devices (IoT, IIoT, Mobile, etc.)
15. Participate in Information Sharing and Collaboration

When you are just starting to build a new cybersecurity strategy, this list can sound daunting. You are probably asking yourself, *How do I prioritize all these? Where do I even start?* These are legitimate questions and ones that a good strategic partner is equipped to help you answer. Listening to experts will only accelerate your efforts by helping you identify which pieces should be offloaded for the greatest efficiency, with less cost, to achieve greater impact

(aka ROI). To realize this ROI, your strategic partnerships should include organizations who truly know cybersecurity and the challenges associated with managing and securing critical infrastructure.

How Should You Start Assessing Risk and Sharing Threat Information?

Let's start with the two controls that require partnerships to be successful: Assessing Risk and Information Sharing (exchanging threat intelligence with others). Both controls rely upon having a strong knowledge base around how attackers are attacking. The industry terminology for this knowledge is what we call Tactics, Techniques, and Procedures, or TTP for short. Knowing the methods and motivations of real-world attacks requires having a pulse on the global threat landscape and how it impacts individual organizations. Working with vendors who offer security-first products and proactive guidance is a great way to gain direct access to this knowledge. Ask your vendors to share insights, and look for vendors who offer regular touchpoints to stay connected with what's happening from one quarter to the next. Threats can change rapidly, and based on the uptick water facilities are seeing in cyber attacks, a regular cadence is important to understanding the size and shape of your threats in real time. Additionally, participating in organizations such as WaterISAC will also give you a great avenue to understanding the threat landscape within the water sector.

Assess Your Risks (#2)

AWWA's fundamental guidance describes the Assess Risk component as "daunting to measure" and goes on to recommend that "consulting firms also provide these services." Assessing risk is one area that can really benefit from an outside perspective. It's easy to get tunnel vision inside an organization, thinking, "No one would bother to attack us, so we have no real cybersecurity risk."

Participate in Information Sharing and Collaboration (#15)

Partnering with a trusted advisor or outside firm can bring a fresh perspective and will give you direct access to lessons learned by other organizations. The fact is, many of the same risks that you may or may not have considered yet have likely already impacted other organizations similar to yours. Learning from their experience with those attacks will strengthen everyone. So, when you are facing new attacks, it's key to also share that information in the right industry-based cybersecurity forums.

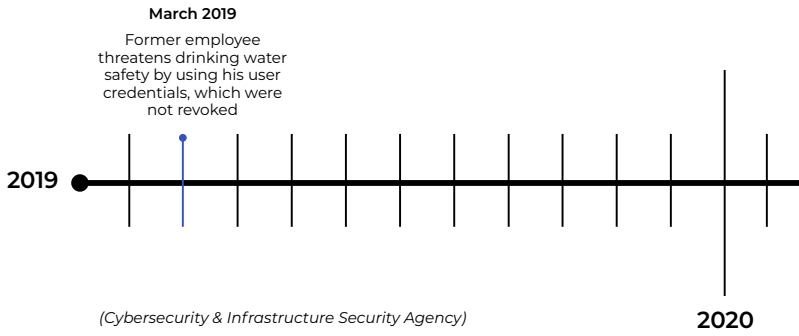
Embrace Vulnerability Management (#7), Implement Threat Detection and Monitoring (#10), Secure the Supply Chain (#13)

Consistent vulnerability management, proactive threat monitoring and tackling complex security challenges like securing the supply chain are all types of security program controls that can be done more efficiently by strategic partnerships with vendors and MSSPs who specialize in security-first services. Offloading these duties are great ways to free up internal resources to focus on your own strategic efforts. For example, leaving around-the-clock monitoring to a dedicated team that can perform this service much more efficiently, expertly, and cost-effectively will keep you from having to hire additional full-time staff, purchase a whole stack of enterprise security tools, find experts who can manage the tools, and keep your people up-to-date with security and tool-based certifications.

The monitoring team you work with will be your front-line defense, whether you choose to keep it in-house or work with a partner. This team will need to operate 24x7x365 to keep a watchful eye on your infrastructure and respond within a few minutes when needed. Our experience has been that the most dangerous cyber criminals generally level their attacks during your team's off hours or holidays, so you can't really afford to just leave alerts to wait until the next business

day. However, having a team who can respond to vulnerabilities and alerts in the middle of the night 24/7 is expensive and costly to do on your own. Forming a strategic partnership with a security operations center (SOC) gives you the best of both worlds: around-the-clock monitoring, but at a fraction of the cost. Going back to our *Security Is a Team Sport* motto, working with a dedicated SOC partner means benefiting from all the insights a partner like CISO gathers from defending attacks across all their other customers. A good SOC will always know what attacks are currently ongoing elsewhere, as well as what steps it takes to stop them. Then, if signs of the same attack are seen in your environment, experts will know from experience exactly what to expect, where to hunt for additional compromises in your environment, and what needs to be done about it. These are elements that you would miss out on by maintaining an internal-only program.

WWS Sector Cyber Intrusions Picking Up Speed



(Cybersecurity & Infrastructure Security Agency)

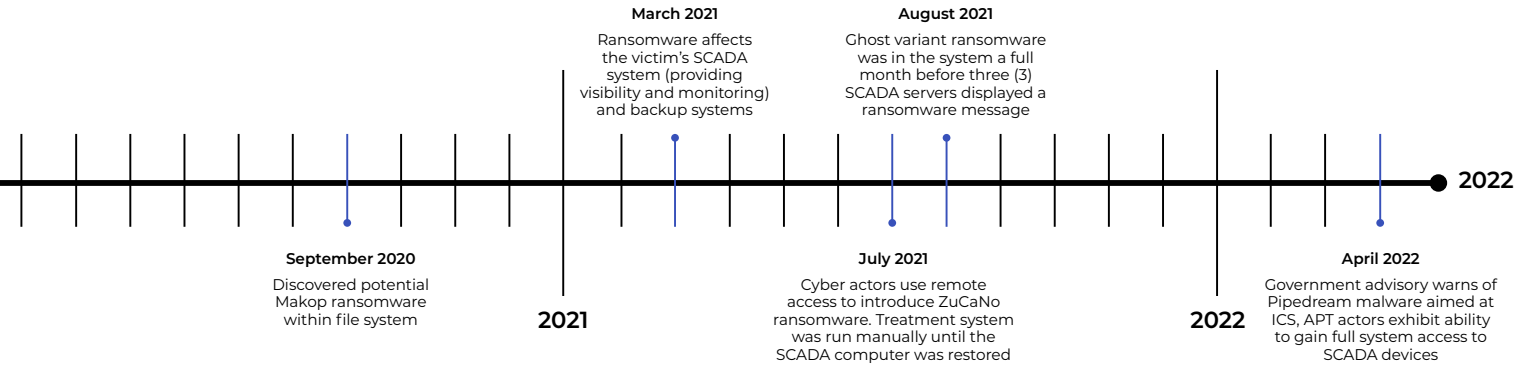
Create a Cybersecurity Culture (#8)

One fundamental that should not be outsourced and should be supported internally is the intentional creation of a culture of cybersecurity. Developing a culture of awareness requires dedication, willingness, openness to new information, and a strong commitment from

Strategic partnership with a security operations center (SOC) gives you the **best of both worlds**: around-the-clock monitoring, but at a fraction of the cost.

leadership. Leadership needs and often desires to be involved, and they are vital to making sustainable change. CISO Global's experts have found that engaging key stakeholders throughout the process is the best way to maintain their support.

- Doing an incident response tabletop exercise? Invite your leadership to attend and give them a role to play, like assigning them to engage as middle management.



- Assessing the cybersecurity risk from a critical vendor for supply chain concerns? Invite your legal council to get their perspective.

The best cultures of cybersecurity are where leadership is engaged in the process, guiding strategic direction, and pushing the organization to prioritize security. Involving leadership to the greatest degree possible will ensure long term success when building and growing your program, because the focus on secure practices will start at the top.

About CISO Global

References

1. American Water Works Association (AWWA): State of the Water Industry '22 Executive Summary

2. CSO: 10 Notable Critical Infrastructure Cybersecurity Initiatives in 2023

3. Cybersecurity Insiders: Heavy Industrial Companies Grapple with Cybersecurity Problems

4. The Hacker News: Industrial Control Systems Vulnerabilities Soar: Over One-Third Unpatched in 2023

A leader in cybersecurity and compliance services, CISO Global brings together expert practitioners and thought leaders to provide tailored solutions that drive cyber resilience. The company's top-tier talent spans geographies, specialties, industries, regulatory frameworks, and focus areas and includes auditors, compliance specialists, certified forensics experts, ethical hackers, security engineers, and around-the-clock analysts.

To learn more, visit www.ciso.inc.

AICPA SOC
aicpa.org/soc4so
SOC 2® Type II Audited