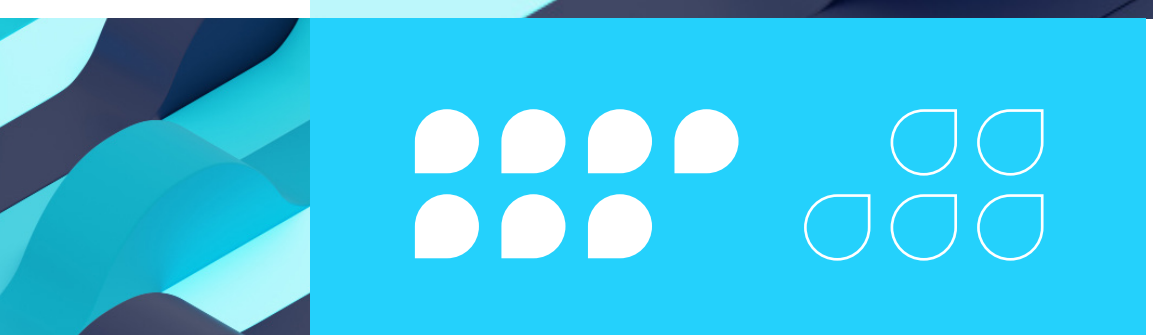
Microsoft

CSC 2.0

ROUNDTABLE SERIES

MULTISTAKEHOLDER INSIGHTS TO ADVANCE WATER AND WASTEWATER INFRASTRUCTURE CYBERSECURITY



EXECUTIVE SUMMARY

Safe and reliable drinking water and dependable wastewater systems are essential to daily life. To improve efficiency and quality of service, water and wastewater systems are increasingly dependent on networked technology – a trend that will only escalate as global digital transformation continues. While these technologies improve the delivery of water and wastewater services, they also introduce new risks. Effectively managing this cyber risk in the United States is particularly challenging because control of water and wastewater infrastructure is distributed among a vast array of over 100,000 unique public and private entities, many of which are small and lack the resources and expertise necessary to mitigate growing threats.

The vulnerability and the criticality of water and wastewater systems make them prominent targets for both profit-seeking cyber criminals as well as geopolitical rivals exploiting a new domain of conflict. Addressing the cybersecurity gaps of this expansive critical infrastructure sector will require robust communication and cooperation across the public and private sectors at every level.

To support this multistakeholder engagement, Microsoft and the Cyberspace Solarium Commission 2.0 (CSC 2.0) jointly hosted a series of roundtable discussions in late 2022 and 2023 on cybersecurity in the water and wastewater sector. Over four virtual gatherings, experts from federal agencies and Congress, as well as from across the water and technology sectors, joined in discussions around (i) threats to the sector, (ii) standards, best practices, and emerging regulations to reduce cyber risk, (iii) international obligations to protect the water sector from cyberattacks, and (iv) how to build cyber resilience across the sector.

Concurrent with the roundtable series, federal agencies, standards bodies, and industry groups have been studying and proposing initiatives to address cybersecurity in the sector. The Microsoft-CSC 2.0 roundtable series, however, was unique in that it brought these communities together to share constructive solutions to shared challenges.

This report contains a summary of those dialogues. The findings across the roundtable series paint a picture of a sector challenged by gaps in cybersecurity risk management alongside a severe lack of resources to address them. We would like to thank the offices of Representatives Jim Langevin and Mike Gallagher as well as Senator Angus King for their support of these roundtable discussions, and the U.S. agencies that participated – including the Environmental Protection Agency (EPA), Federal Bureau of Investigation (FBI), National Security Agency (NSA), Office of the National Cyber Director (ONCD), and National Institute of Standards and Technology (NIST). Together with participants from across the water and technology sectors, as well as from civil society and academia, the discussions surfaced priority recommendations (summarized below) for legislators, relevant U.S. agencies, and the water sector itself.

We hope the discussions facilitated throughout this dialogue series, and the guidance included throughout this report, can underscore the urgency of addressing the challenges and highlight a path forward for investment and cooperation across sectors, stakeholders, and geographies to protect and defend the nation's water and wastewater systems. Moreover, we hope that the recommendations and lessons learned can serve as a valuable reference point for international audiences looking to improve the cybersecurity of their own water infrastructure as well.

CONTENTS

KEY RECOMMENDATIONS

FEDERAL AND STATE LEGISLATORS

- **Resource the EPA, the sector risk management agency** – Addressing the cybersecurity and resilience needs of water critical infrastructure requires national coordination and investment. The Administration needs to request, and Congress needs to support, sufficient funding for EPA to fulfill its obligations as the sector risk management agency for the water and wastewater sector.

- **Expand successful programs that include cybersecurity** – Beyond EPA, other federal agencies, including the Department of Agriculture, have programs that support the resiliency of the water and wastewater sector. Congress should expand these programs to provide cybersecurity support to the sector.

- **Leverage state-level funding mechanisms** – State administrators should use available funding streams like Drinking Water and Clean Water State Revolving Funds[1] to develop and resource comprehensive policies to improve cybersecurity in the water and wastewater sector.

FEDERAL AGENCIES

- **Improve collaboration with sector stakeholders on cybersecurity requirements** – Outside of a regulatory approach, the federal government should work with sector stakeholders to create a joint public-private oversight program to improve the reliability and security of the sector. This program should then develop industry-led cybersecurity requirements for the sector.

- **Fund public-private research on water system industrial control system security** – Historic underinvestment in cybersecurity for the sector has also translated into limited research on cybersecurity for operational technology systems of the water and wastewater sector. The federal government – possibly in collaboration with industry groups – should fund an industrial control system and operational technology water security test bed for cyber-physical security research.

- **Reinforce international expectations** – To deter state-sponsored attacks against the water sector, public attributions of international cyber incidents should always reference when international laws or norms have been violated – especially when attacks have targeted critical infrastructure.

- **Recognize due diligence as a legal obligation:** "Due diligence" is a recognized principle of international law that requires states to prevent their territory from being used as a source of harm to other territories. The administration should join with a number of partner countries that have already recognized that this principle extends to cyberattacks as well, especially when such attacks target critical infrastructure like water systems. This would further encourage governments to take responsibility for malicious activity originating within their borders.

1 https://www.epa.gov/cwsrf; https://www.epa.gov/dwsrf

REGULATORS

- **Allow flexibility to meet cybersecurity outcomes** – Given the diversity of the sector, regulators should allow for flexibility in how each organization allocates resources for improving cybersecurity. Rather than mandating specific steps, funding should allow utilities to identify the vulnerabilities specific to their systems and the appropriate methods to mitigating risk. This outcomes-based approach to regulation ensures that resources are allocated in alignment with the unique needs and challenges of each utility.

SECTOR OPERATORS

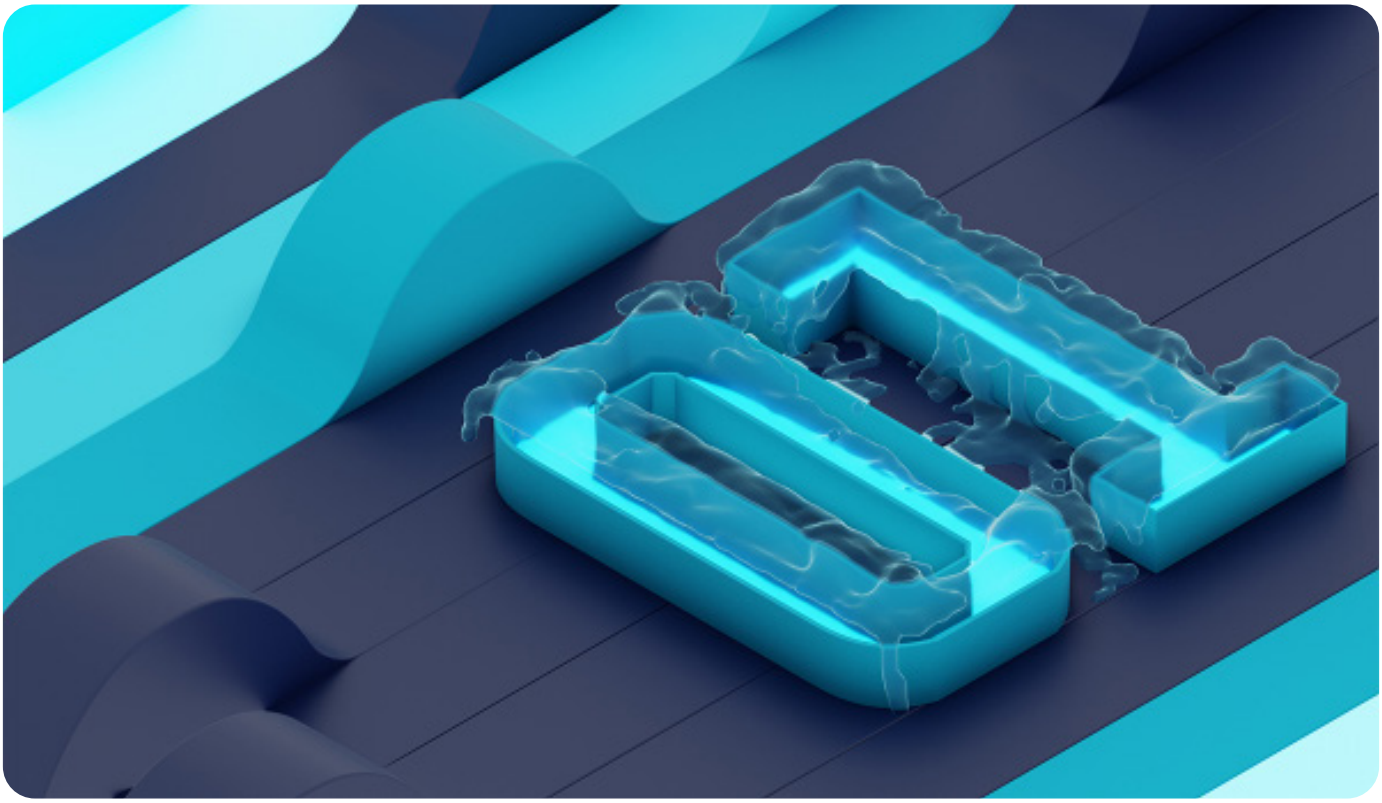
- **Adopt cyber hygiene practices** – The majority of successful cyberattacks continue to leverage phishing attacks and credential theft. To combat this, water and wastewater organizations should improve cyber hygiene by implementing best practices like multifactor authentication (MFA) and protective domain name security practices. Associations and not-for-profit organizations should provide low cost/no-cost assessment and training programs to support this cyber hygiene effort.

- **Build relationships for incident reporting and response** – Before there is a crisis, operators should proactively build relationships and necessary points of contact to both report and respond to significant cyber incidents. This includes establishing a point of contact within a local FBI field office to notify in the case of a significant attack.

- **Participate in information sharing forums** – Operators should participate in the Water Information Sharing and Analysis Center (ISAC). The Water ISAC provides regular reporting on risks, threats, and preparedness in the sector, offering valuable insights and awareness to all participants. It is open to water sector organizations of all sizes, with reduced fees for smaller systems. While some information the Water ISAC provides is publicly available, the curated content in the member newsletter provides convenience and additional value.

- **Build operational resilience** – To build cyber resilience, water utilities should not only seek to keep attackers out but also develop continuity and resilience plans for how to continue to operate through a cyberattack. This means investing in staff training to promote cyber awareness at every level and across departments and designing network infrastructure with proper segmentation, access controls, and intrusion detection systems according to international cybersecurity risk-based standards and best practices.

- **Conduct risk assessments** – A cyber risk assessment is a critical first step for all water utilities in determining vulnerabilities and prioritizing needs to establish a risk-based approach to improving cybersecurity. A number of good cyber risk assessment tools are available, including tools specifically for the water sector, from the EPA, water associations, nonprofits, and private technology and cybersecurity companies.



ROUNDTABLE I CYBER THREATS TO WATER AND WASTEWATER INFRASTRUCTURE

The first roundtable in the series focused on understanding the nature of cyber risk and the threats to U.S. water and wastewater infrastructure, and why it faces such acute challenges in managing cyber risk. In addition to Microsoft and CSC 2.0 experts, this roundtable featured speakers from Congress, the Office of the National Cyber Director, the Federal Bureau of Investigation (FBI), the National Security Agency (NSA), the Water Sector Coordinating Council, and a large, regulated water and wastewater utility.

A RANGE OF THREATS FACING A VULNERABLE SECTOR

Roundtable experts, as well as participants from the audience, all noted that many systems employed across the water and wastewater sectors suffer from a lack of regular maintenance and updates, leaving them especially vulnerable to exploitation. Despite the widespread vulnerability of the sector, however, the number of reported cyberattacks against water and wastewater infrastructure remains low. This could be attributed to a number of factors, including the sector's limited ability to detect and effectively report cyber incidents compared to other targeted sectors such as finance and healthcare.

Speakers were asked about the contingencies that caused them the greatest concern. They warned of two major categories of threats in particular:

- **Criminal actors:** Similar to the wave of criminal ransomware attacks targeting U.S. hospitals, a ransomware attack could exploit vulnerabilities within multiple water systems simultaneously, causing widespread disruptions in water supply, treatment, and distribution.

- **Nation-state attacks:** In addition to causing disruptions on a large or small scale, a nation-state actor could use a combination of cyber and information operations to create the impression of a far-reaching and widespread threat, for example by fabricating 911 emergency calls and generating false social media activity. By combining a cyberattack with influence tactics, an adversary could erode public trust in essential institutions to instill fear and uncertainty in a crisis.

The consensus from the speakers and participants in the discussion was that, today, opportunistic ransomware "gangs" are the most prominent threat actors facing the water sector. Strengthening cyber hygiene practices, implementing network segmentation, and adopting multi-factor authentication are essential steps to begin to mitigate risks posed by these and other threat actors. As the attack surface expands with the integration of new technologies, speakers urged sector operators to incorporate robust cybersecurity controls from the outset.

THE NECESSITY OF COLLABORATION

Speakers noted that responding to these threats also requires a collaborative and multi-faceted approach involving government agencies, industry partners, technology providers, and water system owners and operators. While the EPA is the designated sector risk management agency (SRMA) for the water sector,[2] experts also highlighted the additional following avenues of support.

- *Collaboration between government and industry:* The relationships and collaboration between government agencies such as the FBI and the Cybersecurity and Infrastructure Security Agency (CISA) and water utilities can provide timely information and guidance about emerging threats.

- *Cooperation between large utilities and smaller operators:* By working together, larger utilities can share best practices, offer guidance, and provide resources to smaller operators, fostering a collective approach to cybersecurity.

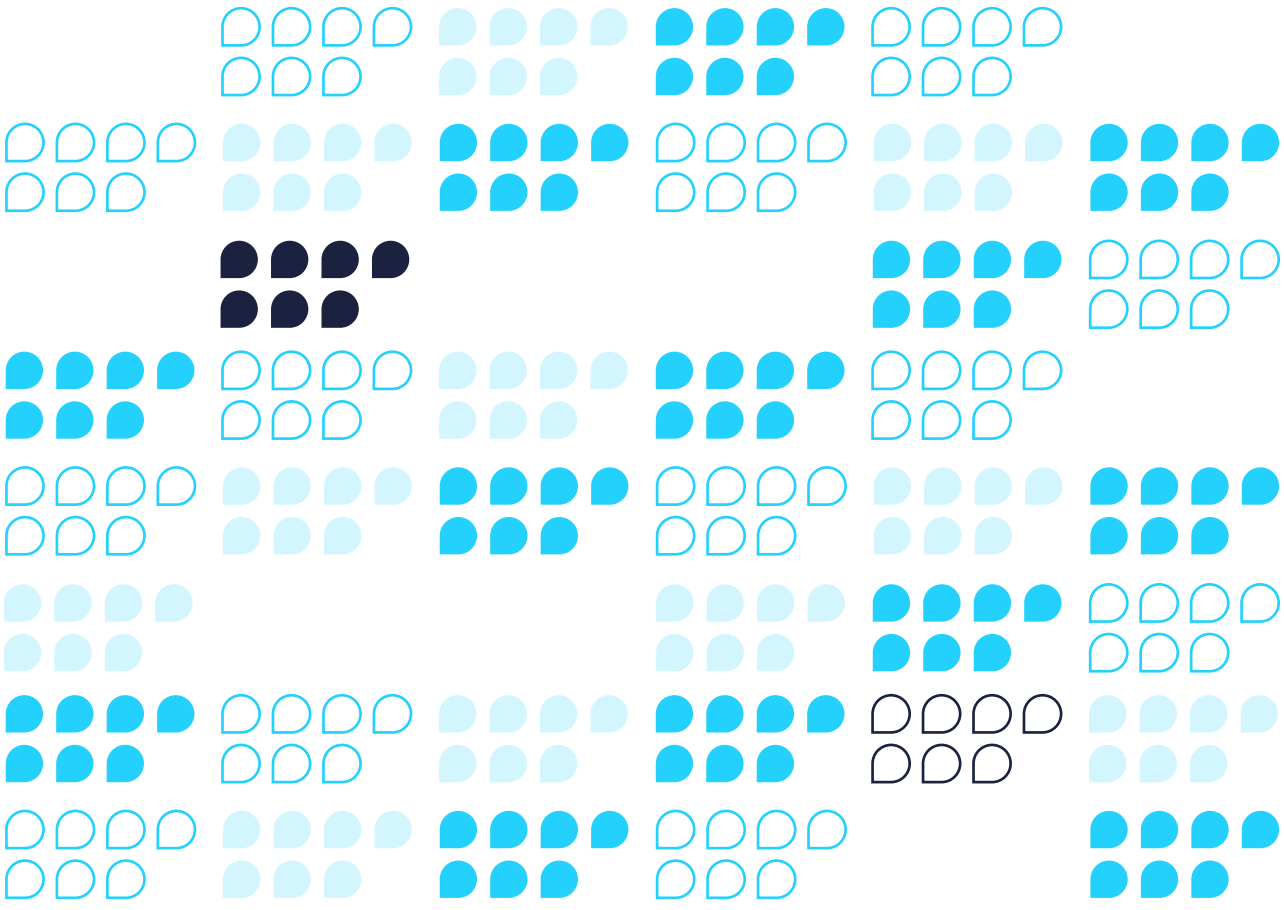
- *Free government services:* Water utilities can also take advantage of no-cost services offered by CISA. Utilities can benefit from services such as vulnerability mapping of their internet-facing assets, which helps identify potential weaknesses that could be exploited by cyber attackers.

- *Federal and state funding:* State and local governments can provide funding to improve cybersecurity in the water and wastewater sector, especially for smaller systems, ensuring they have the necessary resources to enhance their cybersecurity capabilities.

2 https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/sector-risk-management-agencies

Experts in the roundtable discussion emphasized how timely reporting enables agencies like the FBI, CISA, and NSA to take necessary action, including investigation, attribution, and response coordination. For "non-harmful" attacks, water system operators should report incidents through the Internet Crime Complaint Center (IC3) website[3] so that the FBI (and its interagency partners) can monitor criminal trends. For more significant cyberattacks that may have a severe impact on water systems, operators should report directly to their local FBI field office. To this end, building relationships with the local FBI in advance, rather than waiting for a crisis to occur, can facilitate a more effective and efficient response.

Even as experts emphasized that the FBI remains the best initial point of contact during an incident, they also explained how other government capabilities can assist in incident response. In addition to CISA – which serves as the lead agency for asset response and mitigation, the NSA can also contribute to the investigation and mitigation of cyber incidents by tracing leads, determining attribution, and providing insights to inform the response and next steps. Focusing on cyber threats and incident response, this roundtable discussion served to emphasize the necessity of subsequent conversations about how to raise baseline cybersecurity and mature the cyber posture of the sector. These discussions continued in the next roundtable.



3 https://www.ic3.gov/

ROUNDTABLE II REGULATIONS, STANDARDS, AND BEST PRACTICES

The second roundtable focused on emerging regulations aimed at improving the cybersecurity of water and wastewater infrastructure, as well as how the sector is already using standards and best practices and how these latter two can help both regulated and non-regulated utilities improve their cybersecurity. This roundtable featured speakers from the EPA, the National Institute of Standards and Technology (NIST), the Water ISAC, the Association of Metropolitan Water Agencies, and national security think tanks.

THE DRUMBEAT TOWARDS REGULATION

As cybersecurity for water and wastewater infrastructure has increasingly become a national security concern, there have been calls for new regulations. Some of the speakers commented on the EPA's then-newly announced approach to leveraging the existing state-based regulatory model.[4] Regarding regulation and funding, some experts urged that there should be flexibility in how each organization allocates such resources. Rather than mandating specific steps, funding should allow utilities to determine and mitigate the risk specific to their systems.

4 Facing court challenges, on October 11, EPA announced the withdrawal of its memorandum requiring state regulators to include cyber-security assessments as part of their inspections. https://themessenger.com/tech/epa-water-cybersecurity-regulation-withdraw

All of the speakers also discussed how the water and wastewater sector itself is actively engaged in improving cybersecurity measures to enhance the security of the sector. There is currently a lot of focus on adopting and implementing voluntary standards and leveraging available resources to strengthen cybersecurity practices. This not only improves the security posture of water utilities but also prepares for future mandatory regulations. Speakers and participants also suggested the industry as a whole is moving towards a more comprehensive and collaborative approach, where mature utilities are encouraged to support and mentor smaller local utilities.

Even without regulation, experts noted that industry associations and relevant U.S. agencies and standards bodies have developed recommendations, guidance, best practices, and standards that operators in the sector can leverage, including the following:

- *Water ISAC and Water Associations:* The Water ISAC provides regular reporting on risks, threats, and preparedness in the sector, offering valuable insights and awareness to all participants.[5] Both the ISAC and industry associations provide cybersecurity assessment tools and risk management guidance.[6]
- *EPA:* In addition to its regulatory role, as the SRMA for the water and wastewater sector, the EPA provides technical assistance programs and cybersecurity evaluations.[7]
- *NIST:* While many organizations express their willingness to adopt best practices, they may find it challenging to translate standards materials into practical implementation. The National Cybersecurity Center of Excellence, a NIST applied cybersecurity lab, is developing a reference architecture and practical implementation guides for mitigating risk in the sector.[8]
- *Technology and Cybersecurity Vendors:* Speakers and audience members noted that for smaller systems in particular, technology and cybersecurity companies provide free resources.[9] Participants noted in particular the services that Dragos provides through its OT-CERT.[10]

TAKING ACTION: STATE LEGISLATURES AND SECTOR OPERATORS

Roundtable participants pointed out that state legislatures could also play a crucial role in improving cybersecurity in the water sector. States like New Jersey, Florida, and Maryland were specifically noted as taking significant steps to address cybersecurity challenges in the sector through financial support and education and awareness initiatives. Speakers pointed to funding streams like state revolving funds which provide low-interest loans to local governments for water and wastewater system upgrades. State revolving funds have not traditionally been used for cybersecurity, but this may be largely because local governments have not prioritized the cybersecurity needs of these utilities.

5 https://www.waterisac.org/membership

6 See for example: https://www.waterisac.org/fundamentals, https://cybersecurity.awwa.org/, and https://www.awwa.org/Portals/0/AWWA/ETS/Resources/AWWACybersecurityGuidance2019.pdf?ver=2019-09-09-111949-960

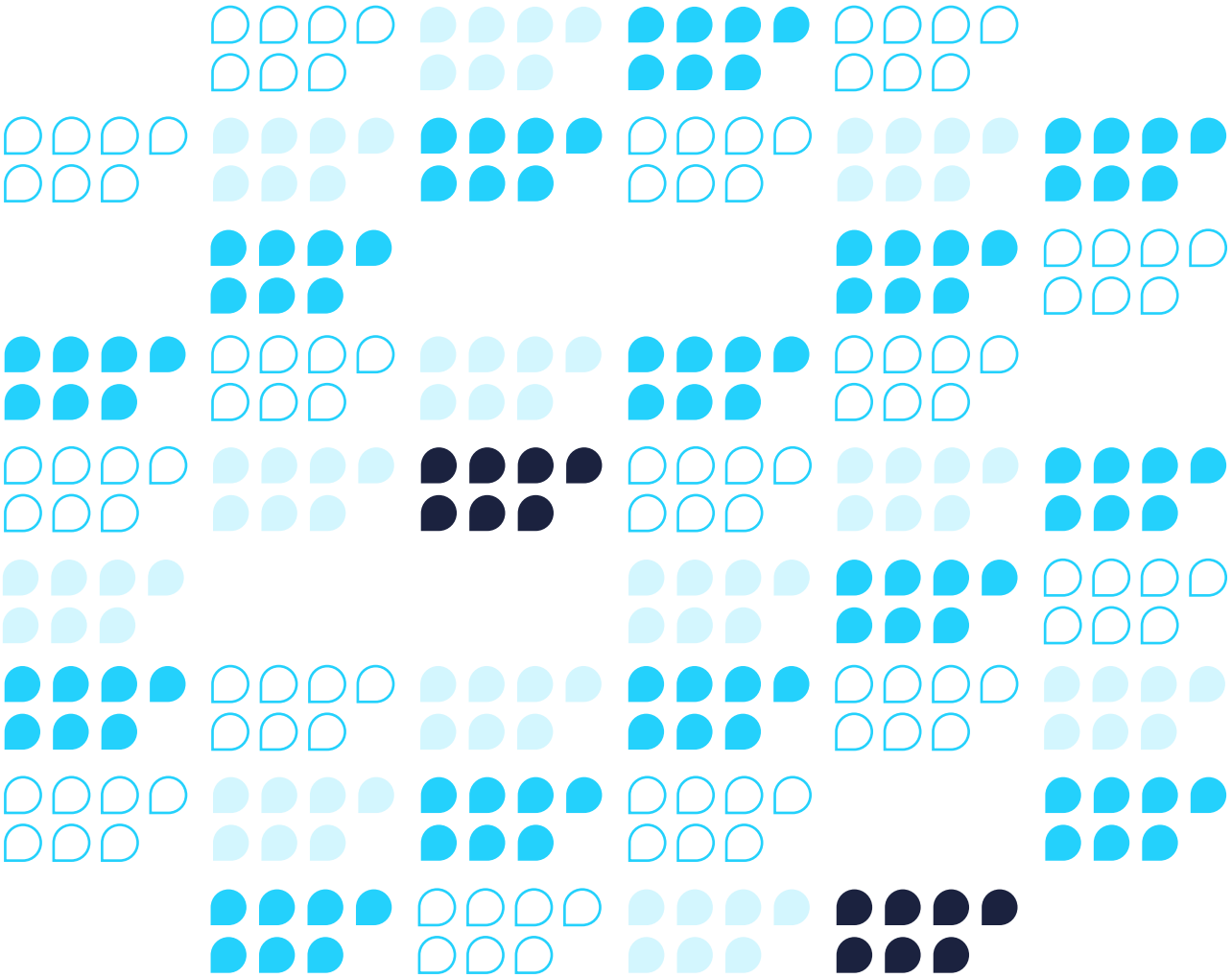
7 See for example, https://www.epa.gov/waterresilience/cybersecurity-assessments

8 https://www.nccoe.nist.gov/projects/securing-water-and-wastewater-utilities

9 See, for example, https://learn.axio.com/free-tool

10 https://www.dragos.com/ot-cert/

The roundtable concluded with some practical first steps for sector operators to begin to implement cybersecurity best practices. Since the majority of cyberattacks are based on stolen credentials that originate from phishing emails, implementing good cyber hygiene will prevent the majority of these incidents. Experts recommended adopting policies like internet browsing whitelisting while noting that it is important to strike a balance, as overly restrictive measures may lead employees to find workarounds that ultimately compromise security.[11] Experts also emphasized the use of multifactor authentication, requiring the use of two or more credentials (a password and a token, for example), so even if malicious actors are able to compromise one credential, unauthorized users will still be unable to access targeted system.



11 Experts also urged the use of Protective DNS service and Domain-based Message Authentication, Reporting & Conformance (DMARC).

ROUNDTABLE III INTERNATIONAL OBLIGATIONS TO PROTECT WATER SYSTEMS

The third roundtable focused specifically on nation-state attacks and international obligations to protect the water sector from these most sophisticated threat actors. This roundtable featured speakers from Microsoft, CSC 2.0, Congress, academia, and U.S. and international think tanks, as well as former government officials. Experts at the roundtable noted that states have a responsibility to refrain from targeting critical infrastructure, including water systems, via cyberattacks, both ethically and under international law. And yet, state-sponsored cyber operations have targeted water infrastructure, including most recently during Russia's war against Ukraine.[12] Experts noted that it is not unreasonable to expect similar attacks targeting critical infrastructure in the United States in the future.

LIMITING STATE-SPONSORED ATTACKS

To address this challenge, experts urged the international community to establish clearer guidelines and stronger mechanisms to hold nation states accountable for their actions in cyberspace. Roundtable participants also suggested that establishing mechanisms for reporting and investigating international cyber incidents targeting critical water systems specifically could also help facilitate collective action and deterrence.

12 https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW10mGC

Speakers offered several specific recommendations to strengthen international expectations:

- *Calling out bad behavior:* Responsible actors should openly criticize and condemn malicious cyber behavior by state actors – especially when targeting critical infrastructure. This kind of public scrutiny can help deter and discourage state-sponsored cyberattacks.
- *Robust attribution:* Promoting accountability starts with accurate and unbiased attribution of cyber incidents. Coordinating attribution statements with other governments can also provide more transparency and accountability.
- *Recognizing the water sector:* Since 2015, all United Nations member states have recognized a voluntary international norm that attacks on critical infrastructure are inconsistent with responsible state behavior online.[13] A follow-up report adopted by the General Assembly in 2021 recognized the water sector specifically as critical infrastructure.[14]
- *Due diligence as a legal obligation:* A recognized principle in other areas of international law, "due diligence" requires states to prevent their territory from being used as a source of harm to other territories. This should apply to cyberattacks as well, especially attacks on critical infrastructure. Several states, including the Netherlands, Germany, Estonia, and Japan, have already endorsed the concept of due diligence as an international legal duty in cyberspace.
- *Multilateral diplomatic efforts:* Ongoing discussions, such as those in the Open-Ended Working Group (OEWG) of the United Nations on information security, provide opportunities to explore how due diligence and other international legal obligations apply in cyberspace. By engaging in these discussions, states can clarify and strengthen international expectations against state-sponsored cyberattacks on water infrastructure.

THE BOUNDARIES OF INTERNATIONAL LAW

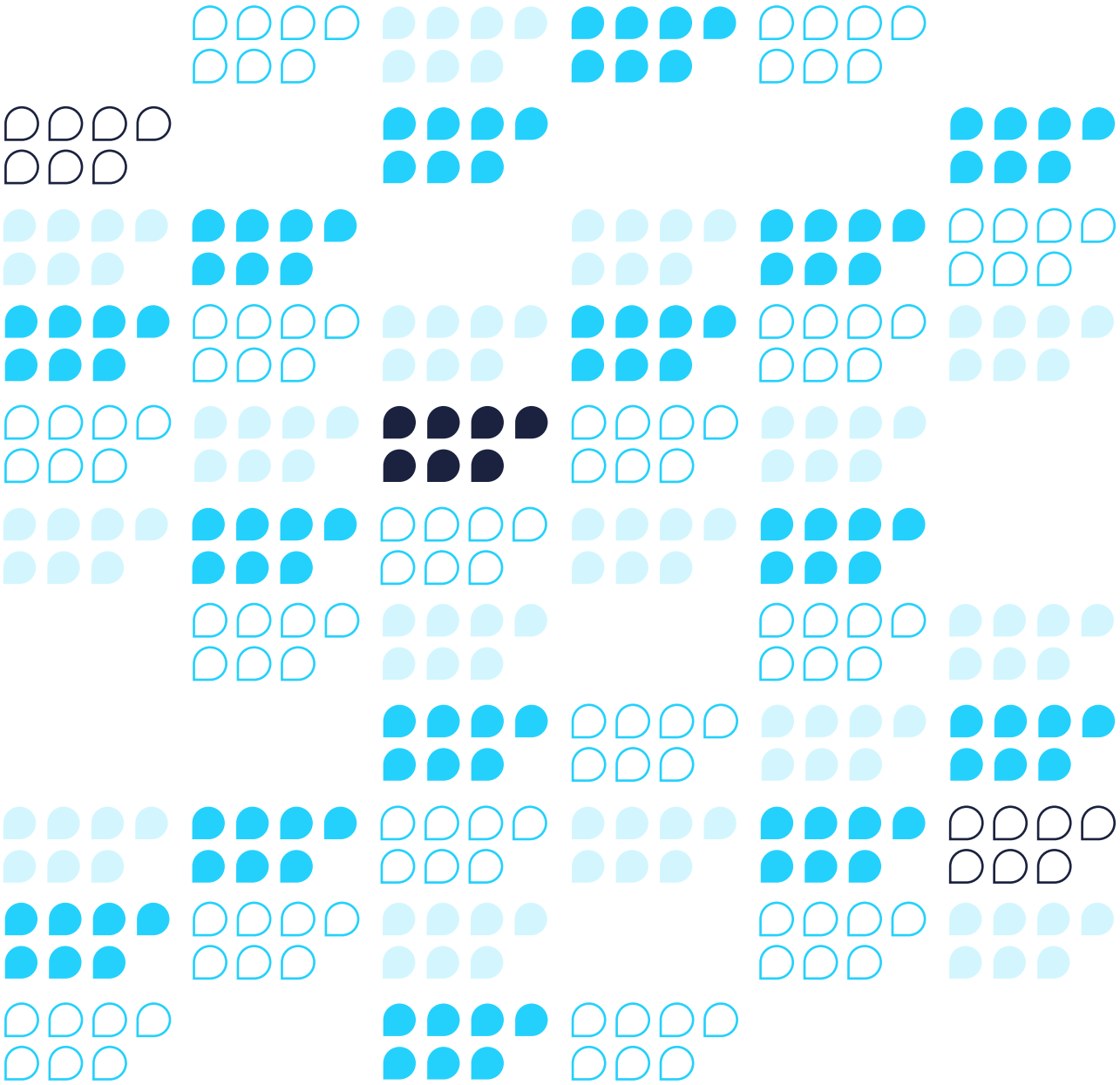
Despite these recommendations, international legal experts at the roundtable pointed out that the application of international law to cyberattacks on water infrastructure by states presents challenges. The existing framework of international law is simply not tailored to address "critical infrastructure" as a protected classification. As a result, targeting a water treatment plant with a cyberattack might only cross the international legal threshold of the "use of force" if it resulted in a public health emergency. Similarly, a ransomware attack disrupting vital water processes might only be considered "coercion" under international law if directed against the state, not an individual water utility.

Experts noted that, unlike other international legal frameworks, international humanitarian law (IHL) does have clear prohibitions against the direct targeting of civilians, but it only applies in times of armed conflict. As most state-led cyber operations have taken place outside of a declared "armed conflict" (with the exception of the ongoing war in Ukraine), IHL has rarely been invoked.

13 https://cyberdefensereview.army.mil/Portals/6/Documents/2022_fall/08_Hogeveen.pdf?ver=BYnHYWAYLrW_PpP4Iljm5A%3D%3D

14 https://front.un-arm.org/wp-content/uploads/2021/08/A_76_135-2104030E-1.pdf

With those considerations in mind, speakers concluded that partner capacity building can and should play a crucial role in supporting cyber defenses and preparing for potential cyber disruptions. In the face of a common set of threat actors, sharing information and collaborating across borders significantly enhances the ability to identify and address cyber threats effectively. The experiences in Ukraine have validated the effectiveness of capacity building efforts undertaken by NATO and the United States since the mid-2010s, as well as cross-sector cooperative efforts, as Kyiv has successfully prevented and mitigated disruptions from Russian cyberattacks.



ROUNDTABLE IV BUILDING CYBER RESILIENCE IN THE WATER AND WASTEWATER SECTOR

The final roundtable in the series explored building cyber resilience across the water and wastewater sectors. This roundtable featured speakers from Microsoft, CSC 2.0, the EPA, the Water ISAC, and the American Water Works Association (AWWA).

KEY ELEMENTS OF CYBER RESILIENCE

Cyber resilience refers to the ability of a system to maintain critical functionality and continue providing uninterrupted services in the face of cyber incidents. Speakers noted that organizations like AWWA have been helping critical infrastructure operators for over 50 years plan for how to persist and maintain operations in the face of traditional threats that could impair services, like severe weather events. Recognizing the importance of technical assistance to cybersecurity and operational resilience, the EPA also launched a technical assistance program, enabling utilities to seek guidance from cybersecurity experts to address specific issues and challenges they may face. Access to such expertise can significantly enhance the resilience of water infrastructure.

Experts recommended that organizations consider the overall risk profile, including cyber risk, based on three elements – threat probability, vulnerability, and consequences. The first element, "threat probability," cannot be changed, just as it is not possible to stop a hurricane. They identified four key components for building cyber resilience in the water and wastewater sector, applicable to entities of all sizes, so that operators can withstand and recover from cyber incidents:

- *Establishing a culture of resiliency.* This involves engaging the right stakeholders within an organization and securing executive buy-in. It is important to assemble a multidisciplinary team consisting of representatives from various departments, including human resources, IT, security, legal, and finance, to identify business continuity and operational resiliency needs.
- *Developing a cyber aware mindset.* Operators must adopt a mindset that it is not a matter of if a cyber breach will occur, but when. This shift in thinking allows organizations to focus on investing across the entire threat cycle rather than solely relying on prevention measures.
- *Understanding resource fundamentals.* In the event of a disruption, water system operators will need to be able to prioritize the restoration of critical assets and infrastructure while effectively managing with limited resources. These operators, thus, need a comprehensive understanding of available resources and how to operate critical systems manually if necessary.
- *Building and adapting a cyber-resilience program.* This involves assessing the current state of cyber resilience within the organization and setting benchmark goals for the future. Speakers noted that the EPA's Comprehensive Procurement Guidelines can provide valuable guidance in this area.[15]

TAKING THE FIRST STEP: A CYBER RISK ASSESSMENT

Experts noted that building cyber resilience in the water sector requires a comprehensive approach that begins with conducting a cybersecurity risk assessment. Various risk assessment tools tailored to the sector's diverse needs are available, such as the sector-specific tool developed by AWWA based on the NIST framework.[16] The EPA has also developed tools to assist in this process. In addition to the above principles, speakers offered specific, actionable steps that operators should take to improve their cybersecurity posture and operational resilience:

- *Asset Inventory and Assessments.* Operators must have a clear understanding of the hardware and software they are operating within their infrastructure. This includes identifying all systems and components, as well as the controls in place to mitigate cyber risks. Conducting regular inventories and assessments will help ensure that all assets are accounted for and properly protected and that operators and decisionmakers understand the criticality of different systems and data and know what to do if they fail.
- *Train staff.* Comprehensive staff training can help ensure that staff at all levels understand their role in the cyber risk management regime. Personnel should understand potential cyber risks, their responsibilities, and how their actions can impact the overall security of the system.

15 https://www.epa.gov/smm/comprehensive-procurement-guideline-cpg-program

16 https://cybersecurity.awwa.org/

- *Maintain a data management profile.* Effective data management is essential for cyber resilience. Operators should establish and maintain accurate profiles of personnel, operational technology systems, and other critical data. This includes documenting access privileges, roles, and responsibilities, as well as implementing proper protocols for data handling and protection.

- *Protect systems from unauthorized access.* Both physical and virtual access to water systems must be protected. Implementing robust access controls and surveillance systems can detect unauthorized entry. Additionally, employing physical security measures such as armed guards at facilities can further enhance protection against potential threats.

- *Implement secure network design.* Implementing a well-designed network can reduce the risk of unauthorized access and limit the impact of potential cyber incidents. Operators should follow baseline controls when designing their networks, ensuring proper segmentation, access controls, and intrusion detection systems.

Roundtable experts pointed out that properly building cyber resilience in an organization can require substantial investment. While a risk assessment provides insights into necessary measures, addressing cyber risks can be costly. Large water utilities may need to invest tens of millions of dollars to overhaul their operational technology systems. Meanwhile, smaller utilities may not have the funds to make the necessary upgrades. Some of the speakers, therefore, encouraged the federal government to support water and wastewater cybersecurity with increased capacity development and funding. These experts noted, however, that the sector has suffered from a historical lack of cybersecurity funding compared to other sectors, such as energy. To ensure the successful implementation of cyber resilience programs in the sector, some of the experts and participants during the roundtable emphasized a need for sustained investment and support from policymakers.

Finally, this last roundtable touched on analysis and recommendations from the Foundation for Defense of Democracies and the CSC 2.0 to strengthen EPA and Department of Agriculture programs for water cybersecurity.[17] Some of the speakers and participants endorsed these recommendations and also emphasized the need to establish a government-industry standards body to ensure the implementation of robust cybersecurity standards across the water sector in a way that is not overly burdensome from a regulatory standpoint but ensures consistent and effective cyber risk management.

17 https://www.fdd.org/analysis/2021/11/18/poor-cybersecurity-makes-water-a-weak-link-in-critical-infrastructure/; https://cybersolarium.org/model-legislative-text-updated/#Water-Sector-Model-Legislative-Texts

APPENDIX

"CERTIFIED CYBER READY" A NEW PILOT FOR WATER UTILITY RESILIENCE

Reflecting on the findings as the roundtable series reached its conclusion, Microsoft and CSC 2.0 sought a way to directly impact the cyber resilience of the sector. Many roundtable participants lamented the resource constraints facing water utilities, and so free training and capacity building became a priority. After reviewing programs offered by for-profit companies and nonprofit organizations, Microsoft determined the Cyber Readiness Institute's (CRI) program was well-positioned to have a meaningful effect on the sector. CRI's Cyber Readiness Program (CRP), a free program geared toward small- and medium-sized enterprises, focuses on foundational lessons, providing policy templates and training on passwords and multi-factor authentication, phishing, software updates, secure file-sharing, and incident response. The program is designed to change behavior and create a culture of cyber readiness.
Together, the three organizations crafted a pilot program to provide up to 200 small- and medium-sized water and wastewater utilities (servicing 501 to 10,000 customers) with foundational cybersecurity training based on the CRP. Additionally, CRI is supplying Cyber Coaches to provide hands-on support to participating utilities throughout their journey. These coaches will help participants complete the program, train their staff, adopt resiliency policies, and develop a business continuity playbook. Participants complete a baseline assessment and a reassessment at the start and end of the program. Upon successful Playbook verification, participants are declared "CRI Certified Cyber Ready."
Further recognizing water and wastewater utilities may have unique needs compared to other small- and medium-sized enterprises, CRI, Microsoft, and CSC 2.0 are prepared to develop additional trainings and services. For this reason, the initiative is split into two phases. The first phase, launched in August 2023, is evaluating the relevance of the CRP content for the water and wastewater sector. The second phase will begin in early 2024 after the three organizations determine what, if any, supplemental content needs to be developed.
When the Office of the National Cyber Director released the National Cyber and Education Strategy last summer, the White House lauded this pilot project noting the important impact the private sector and nonprofit community can have on national cyber resilience. As with this roundtable series, the organizations will publish a report on the findings from this pilot project when it is completed. The data and analysis are hoped will inform critical infrastructure policy moving forward, educating policymakers on the cyber readiness of the nation's critical infrastructure and how the sector's cyber vulnerabilities impact national security and public health and safety.

CONCLUSION

The significance of water systems extends far beyond their immediate impact on drinking water and sanitation, affecting numerous critical sectors reliant on safe and reliable access to water. Disruptions to water functions have cascading effects on agriculture, food production, healthcare, emergency services, and other critical infrastructure sectors. These interdependencies, combined with the distributed ownership and operation of water infrastructure across nearly 100,000 entities, demand a collaborative approach to cybersecurity, bringing together government and sector expertise and resources. The spirit in which speakers and participants shared their analysis, ideas, and recommendations during the Microsoft-CSC 2.0 roundtable series serves as a model for the public-private collaboration needed to protect this most vital of critical infrastructure sectors.


Microsoft
CSC 2.0