GHD Digital

Cybersecurity in water

Overcoming vulnerabilities to build a vigilant, resilient and secure critical water infrastructure

→ Transform for good

According to GHD analysis, about a quarter of global water systems will likely have experienced a cybersecurity breach by 2025.

Introduction

Water is a critical resource for sustaining human life and the global economy. Water systems are considered critical infrastructure that supports essential services such as drinking water, sanitation, irrigation and power generation.

These systems are complex and interconnected, consisting of multiple components such as pumps, valves, sensors, treatment systems and control systems. Any disruption or damage to these systems can have far-reaching impacts on public health, the environment and the economy. In addition, these systems often operate in harsh and remote locations, making them difficult to monitor and secure.

Water systems are often managed by remote monitoring and control systems that rely on diverse data networks, software applications and hardware. While these technologies offer numerous benefits, they also introduce new vulnerabilities that cyber threat actors can exploit.

Attackers can exploit software, hardware and communication protocol vulnerabilities to gain unauthorised access to water systems. They can also launch ransomware, denial-of-service attacks and phishing attacks to disrupt operations or steal sensitive data.

The water sector faces a significant and escalating threat from cyber-attacks as cybercriminals could exploit vulnerabilities to access essential water treatment systems. For instance, there was a 100% increase in malicious techniques used by cyber-attackers to take control of a program or operating system in 2022 compared to 2021[1]. These attacks highlight the need for robust cybersecurity programs to ensure the safety and reliability of water systems. Currently, cybersecurity practices are not widely implemented across many water systems. Despite government efforts to enhance cybersecurity through voluntary measures, progress has been slow in safeguarding the world's crucial drinking water systems. This article explores the challenges of cybersecurity in water and highlights the steps that can be taken to enhance security and resilience.

2030 **US$64 billion**

2022 **US$26 billion**

The digital tidal wave

The global water utility sector expenditure on digital solutions will likely grow from US$26 billion in 2022 to US$64 billion in 2030, a 146% increase. Globally, water utilities will likely spend a combined US$355 billion on digital technology and services from 2023 through 2030. Key drivers comprise the need for improved efficiency, greater sustainability, enhanced customer service, and enabling remote monitoring and control of water systems.

Source: GHD analysis

Technology is driving increasing vulnerability

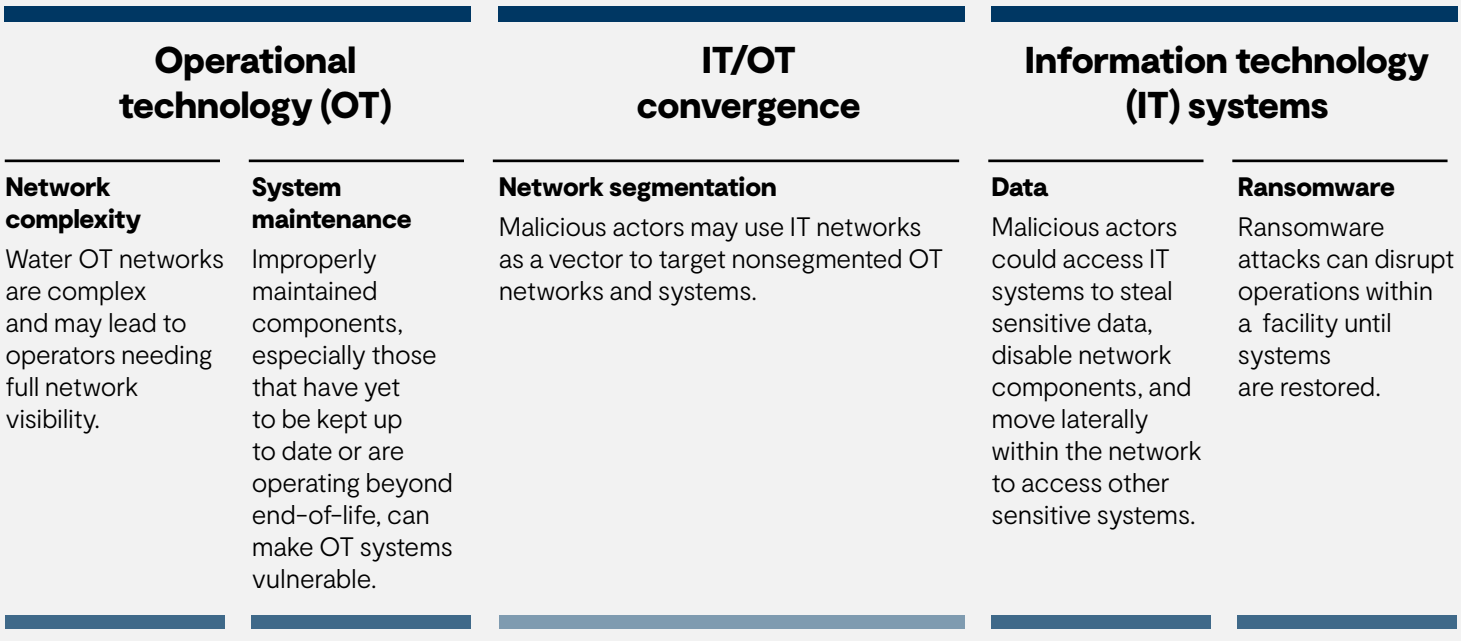
The increasing power of computing and the decreasing size and cost of technology has led to the blurring of the physical and digital worlds.

This convergence of IT (Information Technology) and OT (Operational Technology) makes critical water infrastructure vulnerable to cyber threats (Figure 1).

Specifically, as water utilities increasingly use IoT devices and advanced metering infrastructure (AMI) to collect and transmit data about water usage and distribution patterns, there is an expanding risk that this data could be used to identify individuals or organisations.

As a result, 55.7 billion connected IoT (Internet of Things) devices will likely be in use globally by 2025 [2]. Physical objects such as pumps and valves can now be equipped with digital sensors and controls, which can be connected by common ethernet, making them more accessible to core IT networks and the Internet.

Figure 1: Water networks often have porous IT or OT boundaries, leading to a larger attack surface



Source: GHD analysis and Cybersecurity and Infrastructure Security Agency (CISA).

OT plays a crucial role in the water infrastructure, encompassing the hardware and software systems that monitor and control critical processes, such as water treatment, distribution and management. However, given the increasing interconnectedness of OT systems with IT networks, the water sector has become more vulnerable to cyber threats, as malicious actors can exploit numerous cybersecurity infiltration points (Figure 2). These threats can compromise the integrity, confidentiality, and availability of essential data and operations, potentially leading to service disruptions, public health risks and environmental hazards.

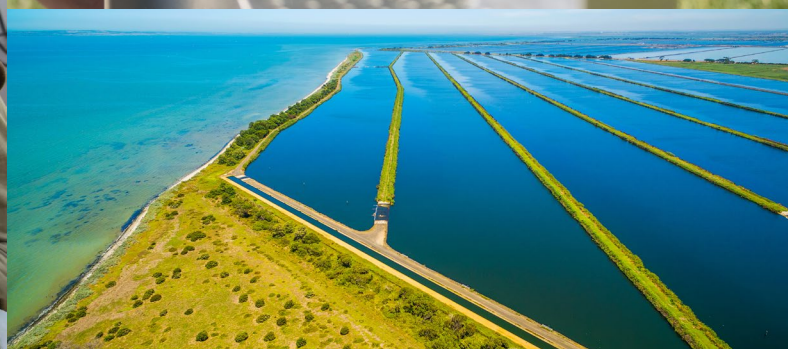
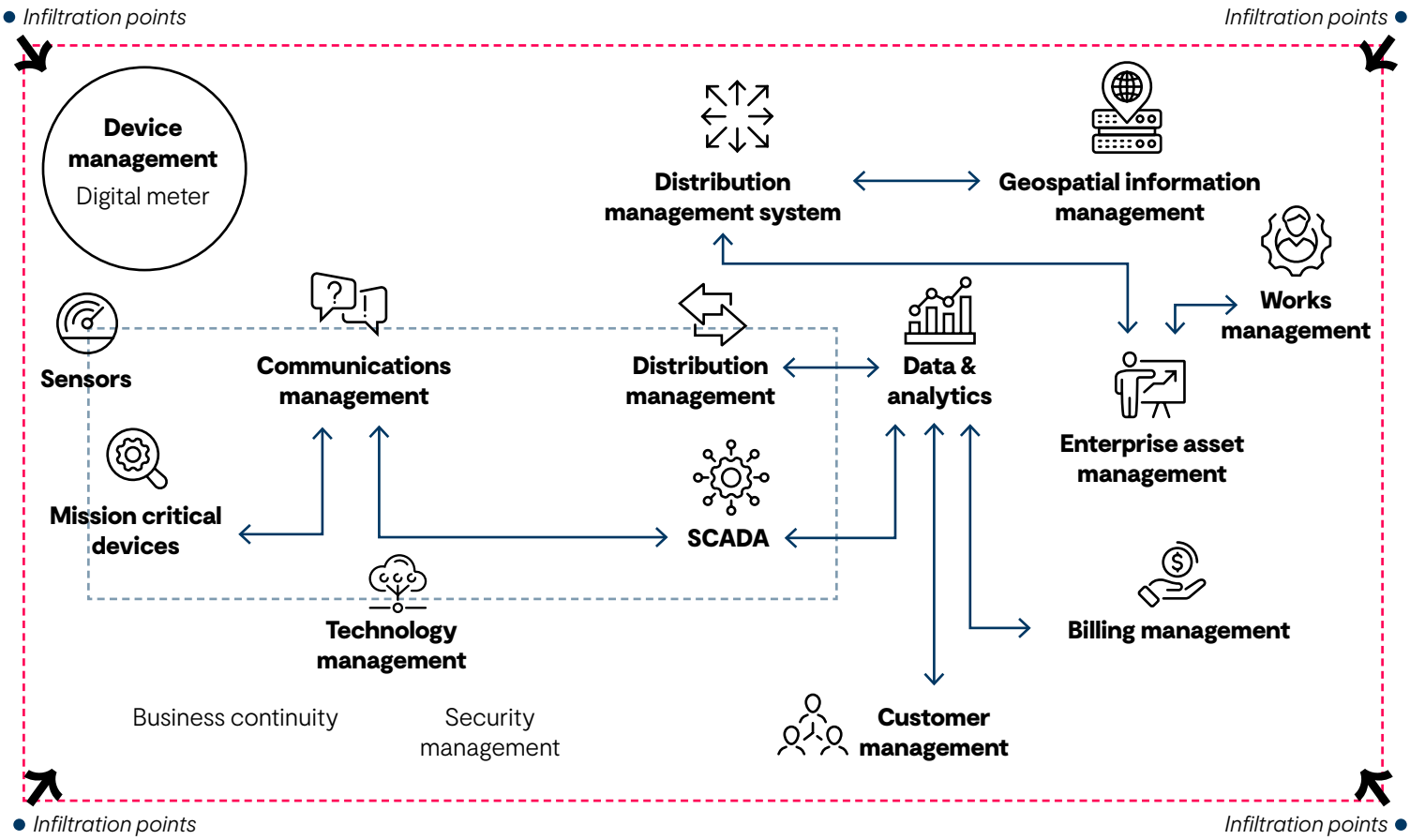


Figure 2: As an integral part of water infrastructure, operational technology (OT) has many cybersecurity infiltration points



Source: GHD analysis

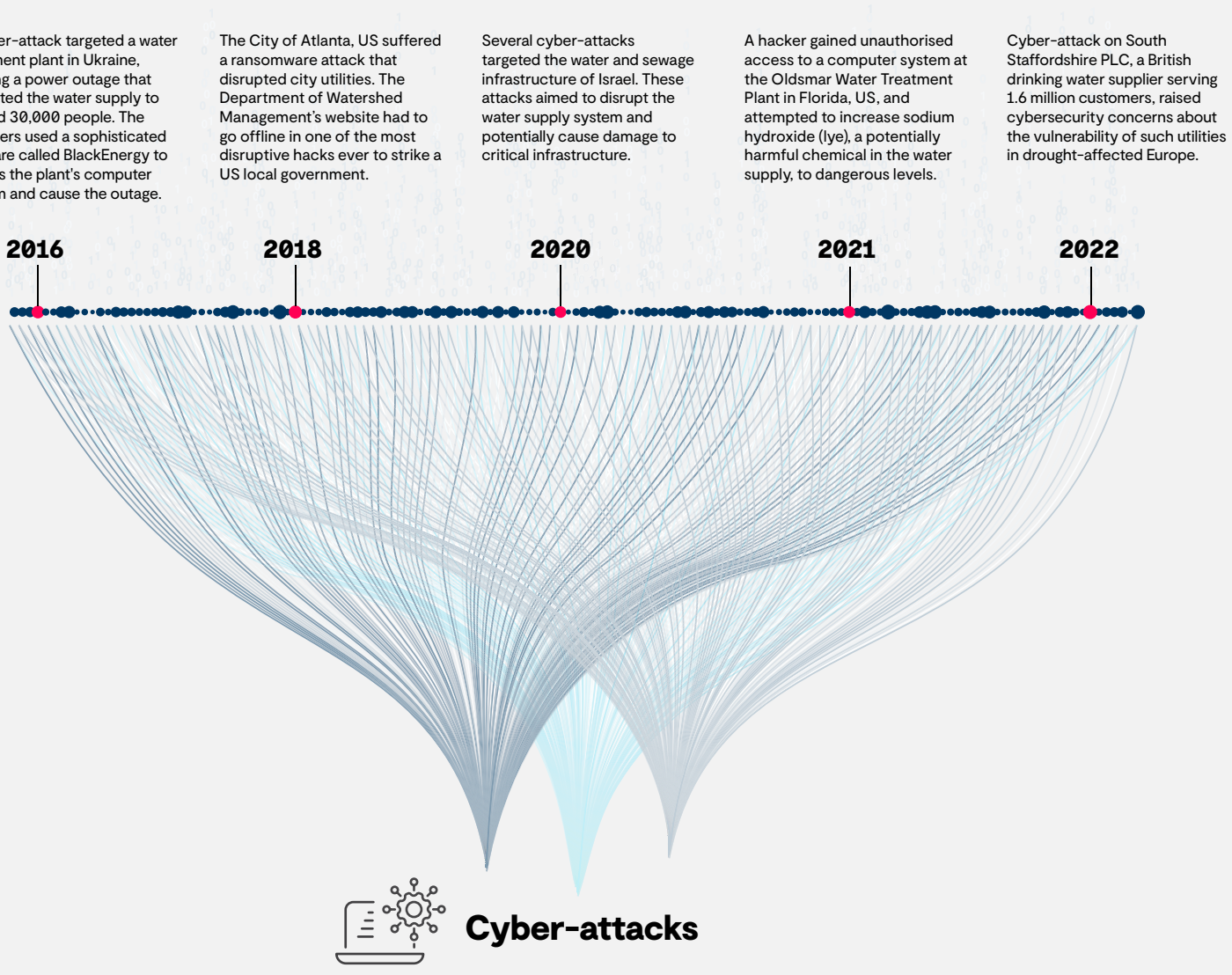
There have been several notable cyber-attacks targeting the water sector in recent years. Figure 3 illustrates some of the major recent cyber-attacks.

These events highlight that cyber-attacks in the water sector are a growing concern and require attention from both water utilities and government agencies to mitigate the risks and ensure the safety and security of our water systems. In the US, under America's Water Infrastructure Act of 2018 (AWIA), the federal government enacted legislation that requires water system operators to address cybersecurity as part of their emergency response plans[3]. This move is part of EPA's expanded oversight of cybersecurity vulnerabilities.

Yet, security measures and investments have not kept pace with the growing concerns. For example, a Water Sector Coordinating Council survey estimates that 38% of water utilities in the US only allocate 1% of their budget to cybersecurity due to limited finances and underestimating cybersecurity risks[4]. Also, according to Water Information Sharing and Analysis Center (Water-ISAC) report, only 23% of utilities surveyed stated they perform annual cybersecurity risk assessment[5].

On average, in 2022, utilities spent just 8.0% of their IT budgets on cybersecurity in North America, compared to 9.9% for all industries[6]. Technology, healthcare and business services led all industries in cybersecurity investment, with 13.3%, 13.3%, and 13.2% of their IT budgets spent on cybersecurity[7]. To effectively mitigate the ever-evolving threat landscape, utilities should be prudent and increase spending on cybersecurity to be at par with industries such as technology and healthcare.

Figure 3: Multiple cyber-attacks have caused disruption to services for water and wastewater systems



Source: GHD analysis

The frequency of attacks and the number of threat actors is on the rise

Water utilities are experiencing a growing number of attempted cyber-attacks, and the frequency of such attacks is rising. While internal threats such as disgruntled employees and partners have been common, rival governments and organised crime groups are becoming more active. Also, hackers with little technical or institutional knowledge are accessing sophisticated tools on the dark web, which operates outside the traditional Internet, compounding the problem. Figure 4 shows the variety of adversaries that threaten water systems and their perceived severity and impact. These threat profiles could vary over time and across geographies.

Figure 4 : Water systems face the highest cyber risk from insiders, rival governments, and organised crime groups

		Impact				
		Risk to life	**Damage to critical infrastructure**	**Business disruption**	**Financial fraud**	**Data theft**
Actors	Employees/ partners	●	●	●	●	●
	Rival governments	●	●	●	●	●
	Organised crime groups	●	●	●	●	●
	Hackers	●	●	●	●	●

Source: GHD analysis

● High ● Moderate ● Low

Organisations operating in the water sector should prioritise the potential physical harm to humans and the environment as malicious actors could exploit vulnerabilities in cyber-physical systems to cause intentional harm or fatalities.

Increased risks require a holistic cybersecurity approach

Enhancing cybersecurity in water requires a multifaceted approach that addresses people, process, and technology issues. Below are the key steps that should be undertaken to improve cybersecurity in water (Figure 5).

Figure 5: Moving from now to next-level cybersecurity in water

Source: GHD analysis

Identify and monitor critical water assets

Water utilities should take inventory and monitor their critical infrastructure assets to enhance real-time information-sharing, detection, and response capabilities for their OT. They should also collaborate with other organisations in the water sector, such as government agencies, regulators and industry associations, to share information on emerging threats and best practices for cybersecurity. Such collaborative efforts between the water ecosystem can result in the development and deployment of technology tools that provide visibility into water systems while ensuring data anonymity and privacy protection for companies.

Conduct risk assessments

Water utilities should conduct regular risk assessments to identify potential vulnerabilities, threats, and impacts to their systems. These assessments should consider internal and external threats, such as cyber-attacks, natural disasters and equipment failures. Also, developing a incident response plan that includes procedures for responding to cyber-attacks can help minimise the impact of an attack and enable the water utility to resume normal operations quickly.

Establish minimum security standards

To ensure the security of critical water infrastructure, organisations, including governments, technology companies, and third parties, must establish minimum security standards tailored to their function and the impact of potential losses. Governments should consider regulating the cybersecurity standards of all IT products and launch cyber hygiene campaigns to educate citizens about common threats and how to protect themselves. And water utilities should implement multifactor authentication, zero-trust architectures and cybersecurity training for all users. These small changes can have a significant impact.

Implement security controls

Water utilities should implement various security controls to protect their systems from cyber threats. These controls include firewalls, intrusion detection systems, access controls, encryption and network segmentation. Furthermore, organisations can leverage analytics and visualisation to audit their real-time cyber risk profiles. Analysts can collect relevant data and use an analytical model to create a custom real-time dashboard that tracks cyber risk, providing real-time visibility into a company's cyber risk profile.

Continuously monitor and detect vulnerabilities

Water utilities should implement continuous monitoring and detection capabilities to identify and respond to security incidents as they occur. Deploying real-time monitoring and detection systems can help detect cyber-attacks early and enable a rapid response to mitigate the damage. This can involve using security information and event management (SIEM) systems, network traffic analysis and threat intelligence feeds.

Invest in training and development

Water utilities should provide training and awareness programs to their staff to ensure they understand cybersecurity risks and best practices. Training employees on cybersecurity best practices and raising awareness of the risks of cyber threats can help prevent accidental or intentional security breaches. This can include training on password management, social engineering and phishing. In addition, learning efficiencies can dramatically reduce the cost and time needed to integrate cybersecurity.

Developing and implementing a cybersecurity program is crucial for ensuring the secure and resilient operation of water systems, protecting against cyber threats that could compromise public health and safety. And implementing cybersecurity measures in the water sector requires a comprehensive and multifaceted approach that involves technical measures, employee training and strong security culture. By implementing these measures, water utilities can better protect against cyber threats and ensure the safety and security of our water systems.

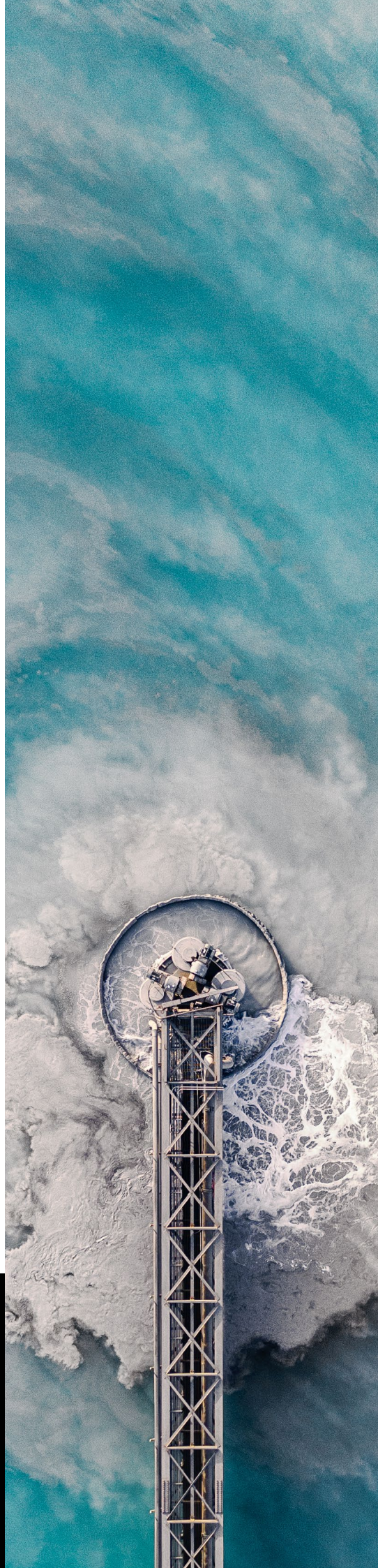
Conclusion

Protecting water systems

Cybersecurity in water is a critical issue that requires attention and investment from water utilities, government agencies and other stakeholders. The risks posed by cyber threats are significant, and the consequences of a successful attack can be severe. Water utilities, therefore, should demonstrate the need for increased cybersecurity measures to protect critical infrastructure and ensure the safety and security of our water systems.

Water utilities must strengthen their cybersecurity defenses and be prepared to respond quickly and effectively to cyber threats. Organisations should establish specific cybersecurity programs and operating models aligned with the water sector and its critical assets. This includes developing and deploying processes that help address specific challenges and deliver, monitor and maintain robust cybersecurity measures.

By implementing robust cybersecurity measures, conducting regular risk assessments and promoting a culture of security awareness, organisations can enhance their resilience and protect the safety and reliability of their systems.



1. IBM, "X-Force Threat Intelligence Index 2023".
2. IDC, "Future of Industry Ecosystems: Shared Data and Insights", January 6, 2021.
3. Addressing Cybersecurity Risks to Community Water Systems under the America's Water Infrastructure Act of 2018
4. American Water Works Association, "Water Sector Cybersecurity Risk Management Guidance", 2019.
5. Water Sector Coordinating Council, "Water and Wastewater Systems: Cybersecurity – State of the Sector", 2021.
6. IANS, "2022 Security Budget Benchmark Report", November 1, 2022.
7. Ibid.

Respond quickly and effectively

GHD Digital

Authors and contacts

Sunil Sharma
Connected Infrastructure and Cybersecurity Leader, GHD Digital
E: Sunil.SHarma@ghd.com
P: +61 2 92397957

Anne-Marie Kirkman
Global Program Lead-Future of Water, GHD
E: Anne-Marie.Kirkman@ghd.com
P: +61 2 92397058

Together with our clients, we are thinking and doing things differently to meet the challenges of digital disruption head-on.

With a sharp focus on the future, we're committed to helping you pre-empt and prepare for what's next.

ghd.com/digital