Sponsored by

FORTINET

2024 Cybersecurity in Water Management Facilities Report

Addressing the growing threat of cyberattacks on America's water supply and wastewater utilities

WASTEWATER DIGEST

WaterWorld

Table of Contents

Executive Summary

In March 2024, the U.S. Environmental Protection Agency (EPA) and the White House issued a warning to state governors, alerting them of the need to protect water and wastewater systems from ongoing cybersecurity threats. Two drinking water-related cyberattacks prompted the EPA to ask states to provide plans to decrease the risk of attacks on water and wastewater systems within their jurisdictions.[1]

These weren't isolated cases. As the prevalence, speed, and impacts of cyberattacks on America's water supply and wastewater utilities increase — regardless of the origin and target — utilities and agencies are allocating investment, time, and effort to thwarting the bad actors behind the attacks.

The potential threats are real, targeted, and aggressive. Hackers may be able to tamper with controls, interfere with chemical treatments, and disrupt water flows. In January, for example, Russian hackers remotely accessed a water tower in the town of Muleshoe, Texas.[2] This was the first-ever disruption of a U.S. drinking water system by Russia, and it led to a state of emergency being declared as the tower overflowed with thousands of gallons for almost an hour.

A survey conducted by Endeavor Business Intelligence on behalf of Fortinet revealed interesting findings from water and wastewater professionals. Since 2021, utilities have put more cybersecurity controls in place, with increases in every type of security control. They're investing in network visibility, for example, and planning to adopt a larger range of security controls. Securing remote access remains a top priority for most utilities as the bad actors become more sophisticated and intrusive. Overall, cybersecurity responsibilities haven't changed much between 2021 and 2024, with the CISO/VP of IT security, supervisory control and data acquisition (SCADA) leader, instrumentation director, and head of operational technology most likely to cover this job function.

The top cybersecurity concerns also remained largely the same, with the key areas of concern including threats to population/public health, service interruptions, and compliance issues. On the cyberattack front, water and wastewater utilities are most worried about ransomware and malware/phishing, both of which were also key areas of concern in 2021.

Meanwhile, water utilities looking to improve their cybersecurity technology face resource, expertise, and ownership challenges. Some blame inadequate funding as a primary roadblock, while time spent running current operations, unclear use and operation of cybersecurity tools, and no clear ownership of the responsibility are also impeding progress on the cybersecurity front.

[1] californiawaterviews.com/white-house-issues-dire-warning-regarding-drinking-water-supply-and-wastewater-system-cyberattacks
[2] dailymail.co.uk/news/article-13337445/russian-attack-cyber-cyberattack-texas-town-water-tower.html

Executive Summary

On a positive note, water and wastewater utilities clearly recognize the challenge, and they're giving cybersecurity a greater priority. They are also planning to make more investments in cybersecurity technologies over the next two to five years. Reported intrusions, increased overall awareness of the cybersecurity problem, and new regulations on water and wastewater utilities are the key drivers for these new initiatives.

As cyber risks continue to intensify and proliferate, cybersecurity has become a top priority for technology investment. Utilities plan to invest in a broad range of cybersecurity measures to improve the security and safety of their operations.

Fortinet surveyed water utility leaders during the second quarter of 2024 to understand water utilities' status and future needs for improved water system cybersecurity.

Introduction: Attackers are Working Faster and Having a Bigger Impact

Water systems and treatment plants are vital lifelines for our communities, but these facilities are also increasingly vulnerable in the digital age. Hackers bent on disrupting critical infrastructure may target the nation's water supply, knowing that the systems that run them are not always modernized and protected by advanced cybersecurity measures.

The survey reveals water utility leaders' heightened awareness of these threats and willingness to invest more time, effort, and money into safeguarding the nation's vital water infrastructure. Key areas of concern include ransomware attacks, malware/phishing, physical attacks, and unintentional "insider" threats.

Respondents are experiencing more cyberattacks overall, with 33% reporting at least one attack in the last 12 months, compared to 22% in 2021. Exposure to cyberattacks has increased slightly, with smaller utilities more concerned than ever about potential cyberattacks. Moreover, U.S. EPA estimates that 70% of U.S. water systems "do not fully comply with requirements in the Safe Drinking Water Act and that some of those systems have critical cybersecurity vulnerabilities, such as default passwords that have not been updated and single logins that can easily be compromised."[3]

Today's cyberattacks are fast, targeted, and impactful. In researching how long it takes a new vulnerability to move from initial release to exploitation, Fortinet's most recent numbers show that cyberattacks started on average 4.8 days after new exploits were publicly disclosed. In fact, during the second half of 2023, attackers increased the speed with which they capitalized on newly publicized vulnerabilities within the aforementioned 4.8 days, versus a previous 8.4 days during the first half of the year.[4]

Fortinet says 44% of all ransomware and wiper samples (malware that deletes or destroys an organization's access to files and data) target industrial sectors like energy, healthcare, manufacturing, transportation and logistics, and automotive. With water and wastewater utilities facing increasing cyber risks, these organizations must understand their security postures and apply best practices to defend their systems.[5]

This survey examines these trends and opportunities to help water utilities benchmark their current cybersecurity capabilities and develop future-focused strategies. It also compares and contrasts with a similar survey Fortinet conducted in 2021 to assess progress and identify remaining challenges in water utility cybersecurity.

[3] epa.gov/newsreleases/epa-outlines-enforcement-measures-help-prevent-cybersecurity-attacks-and-protect
[4] finance.yahoo.com/news/fortinet-threat-research-finds-cybercriminals-130000030.html?guccounter=1
[5] Ibid.

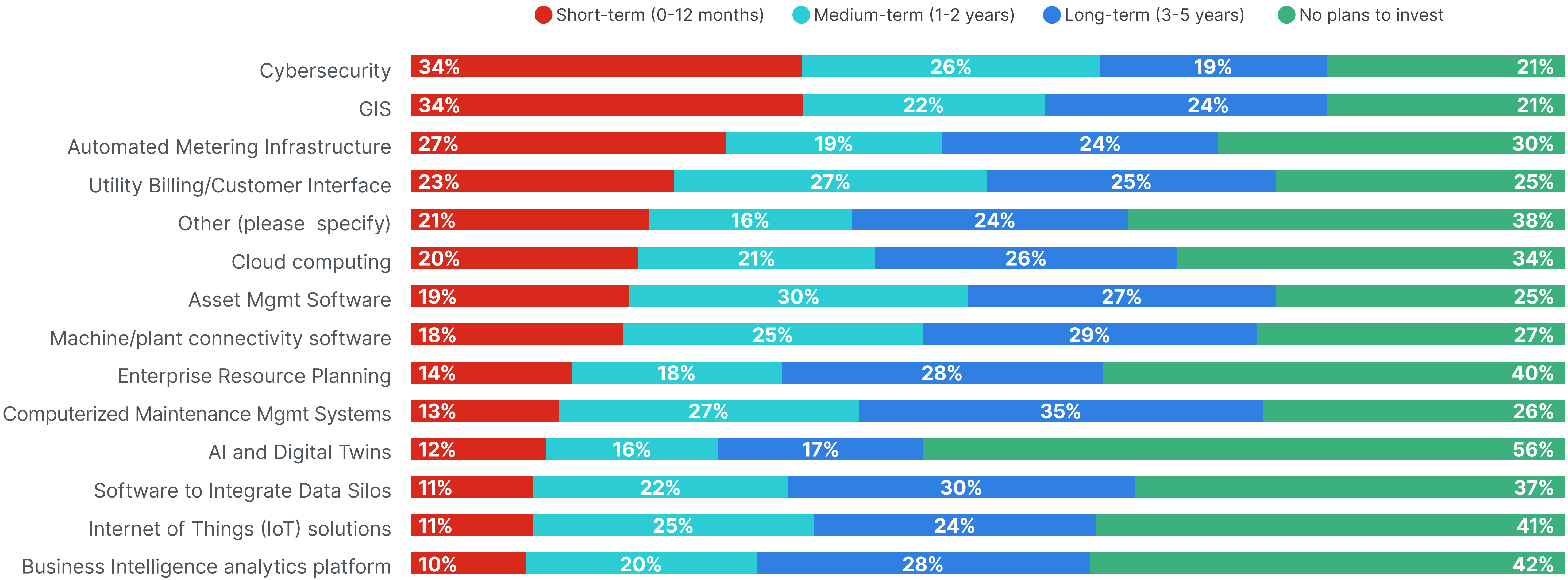
Tech Adoption by U.S. Water and Wastewater Utilities

In 2021, most water and wastewater utilities were investing in cybersecurity, geographic information systems (GIS), asset management software, automated metering software, and computerized maintenance management systems. This focus has shifted slightly over the last three years, with the top technologies that respondents' organizations plan to invest in over the next two years being cybersecurity (60%), GIS (56%), and automated metering infrastructure (56%). (See Figure 1.) Over the longer term, utilities have their sights set on adding more computerized maintenance management systems, software that eliminates data silos, machine/plant connectivity software, and business intelligence analytics platforms to their technology stacks.

At the other end of the scale, 56% have no plans to invest in emerging technologies like artificial intelligence (AI) and digital twins. The timeframes for tech implementation range from short-term (0-12 months) to long-term (3-5 years), falling in line with expected capital expenditures. This suggests they are being incorporated into future capital investments that will take years to complete. While the urgency of cybersecurity is clear, the financial challenges may be a barrier, leading utilities to seek creative approaches in financing or funding digital and cybersecurity efforts by including them in larger capital projects.

Tech Adoption by U.S. Water and Wastewater Utilities

Figure 1: In which areas of technology does your agency/organization plan to invest or improve over the following timeframes?



The top technologies that respondents' organizations plan to invest in within the next two years were GIS (43%), cybersecurity (42%) and asset management software (37%). A third (34%) were not planning to invest in AI and digital twins.

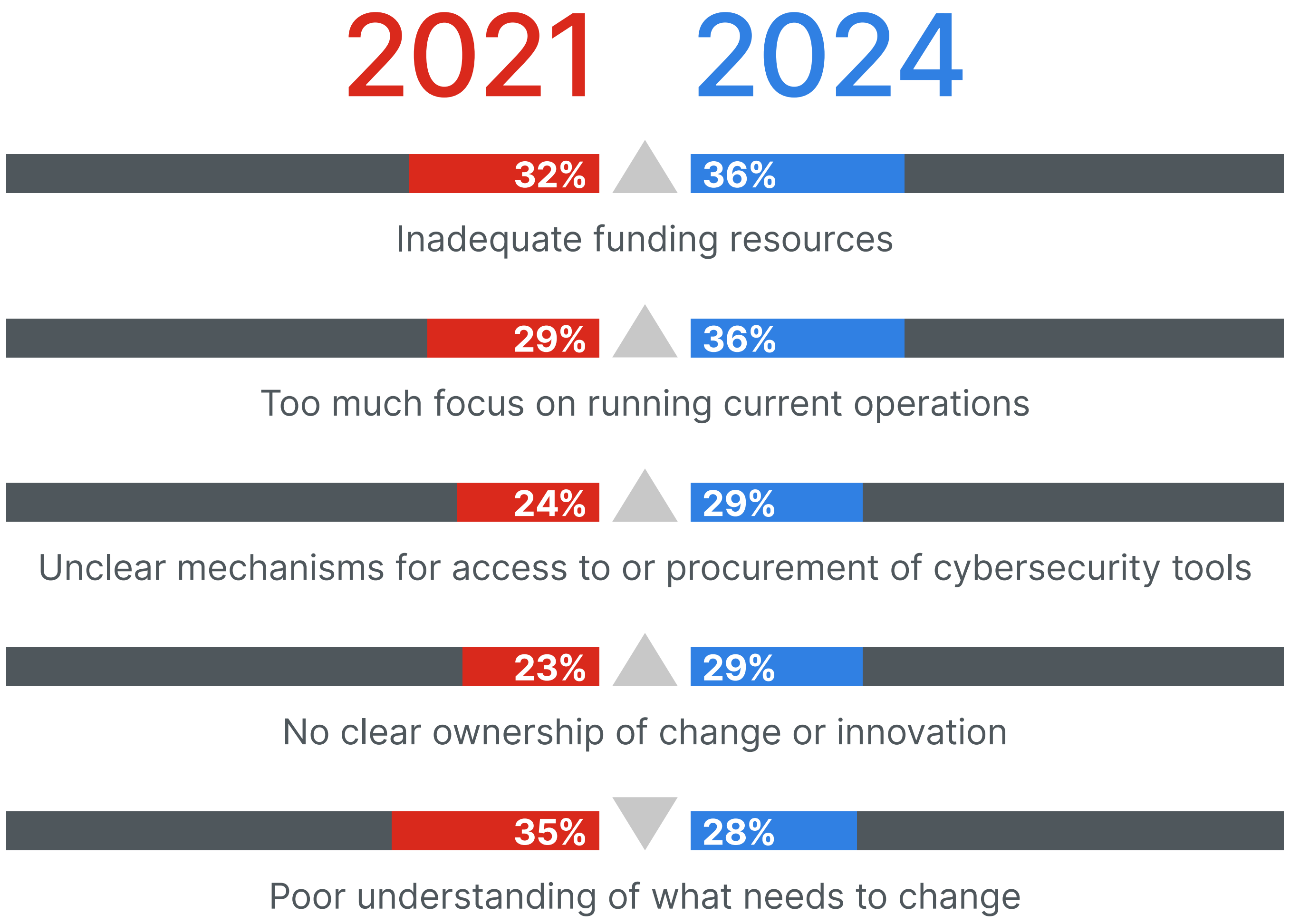
Tech Adoption by U.S. Water and Wastewater Utilities

Challenges for improving technology have shifted since 2021, with inadequate funding resources being the primary roadblock for 36% of utilities (versus 32% in 2021). There's also too much focus on running current operations (36% versus 29% three years ago); unclear mechanisms for access to or procurement of cybersecurity tools (29% versus 24% in 2021); no clear ownership of change or innovation (29% versus a previous 23%); and a poor understanding of the necessary changes (28% versus 35% in 2021). (See Figure 2.)

Agency or utility size plays a role in cybersecurity investment. For example, 59% of organizations with fewer than 25,000 customers plan to invest in cybersecurity, while only 5% of those with 100,000 customers are planning such investments. When it comes to automated metering software, 69% of smaller utilities want to improve or add these capabilities, 25% of midsized providers (25,000-100,000 customers) have such plans in place, and just 6% of large utilities are making these moves.

Based on the survey results, it's clear that smaller utilities want to add these technologies while larger utilities already have these solutions in place. Another interesting inference relates to the maturity of cybersecurity when compared to automated metering infrastructure. Automated metering infrastructure has been adopted by utilities for over a decade; meanwhile, discussions on cybersecurity for water systems have really taken flight in the past two to three years. The

Figure 2: Which of the following are challenges to your agency or organization's progress when it comes to improving your cybersecurity technologies and systems?



Challenges for improving technology have shifted since 2021, with inadequate funding resources (36%) and too much focus on running current operations (36%) emerging as the top challenges for respondents in 2024.

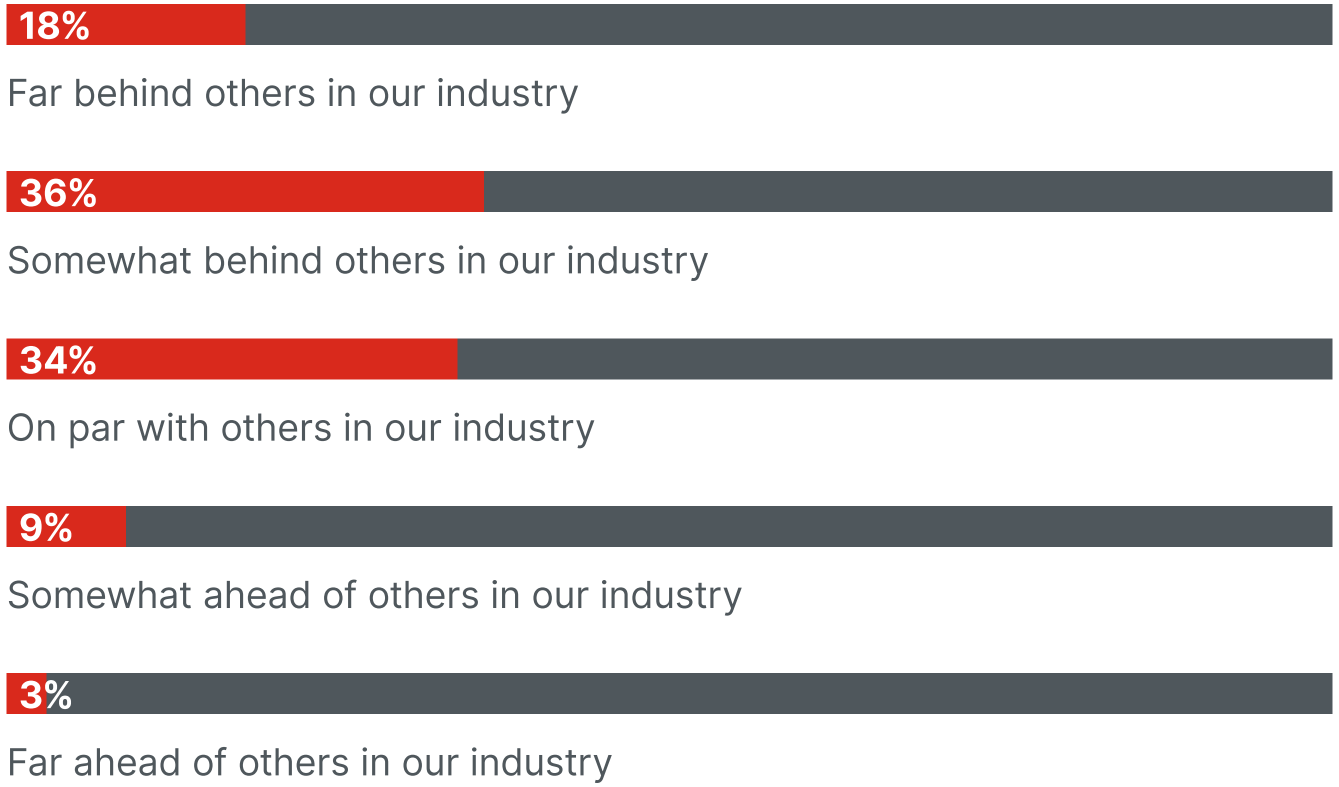
Tech Adoption by U.S. Water and Wastewater Utilities

difference between plans to invest in these two areas for small utilities is only 10 points apart, which shows there is a sense of urgency around cybersecurity. Mature as a discipline, cybersecurity remains under-adopted by the water and wastewater sector. Smaller utilities have plans to invest in critical operational capabilities, with nearly as many anticipating more investments in cybersecurity.

When asked to describe their agency or organization's adoption of digital transformation technologies compared to others in the industry, 34% of respondents felt that their organizations were on par with others, while most respondents (52%) said they are behind on digital transformation. (See Figure 3.) This speaks to water systems' sentiments regarding their maturity level with cybersecurity and suggests they feel they are falling behind. The municipal water market is notoriously slow to adopt new technologies or to incorporate changes. No utility wants to be front page news with a crisis because they were a pioneer, and given these results, it appears cybersecurity may be another casualty of that conservative culture of change.

Analyzing the survey results by organization size, it's clear that smaller utilities are in catch-up mode on the digital transformation front. Nearly all (95%) of those with fewer than 10,000 customers say they're behind; in context, this makes sense. Many of these small utilities have only one or two people to handle all of public works. One person may run the drinking water plant and the wastewater

Figure 3: How would you describe your agency or organization's adoption of digital transformation technologies compared to others in your industry?



94% of large organizations with more than 100,000 customers feel they are on par with others or ahead of the digitalization curve, suggesting these larger systems have the teams and resources to keep on top of the latest issues for cybersecurity.

plant. That same person often also mows the grass for the parks and fills potholes on city streets. Within this context, it comes as no surprise that they feel behind in terms of digitalization, as these small utility operators, owners, and managers are often overworked.

Meanwhile, 42% of utilities with 10,000 to 25,000 customers feel they are behind, and 57% of organizations with 25,000 to 100,000 customers say they feel this way. Just 6% of large organizations with more than 100,000 customers feel like they're behind the digitalization curve, suggesting these larger systems have the teams and resources to keep on top of the latest issues for cybersecurity.

Addressing Looming Cyberthreats

Cybersecurity responsibilities haven't changed much between 2021 and 2024 (chart not shown), with 32% of respondents saying their head of information technology handles this aspect of their businesses — up from 29% in 2021. The remaining percentages stayed largely the same, with the CISO/VP of IT security, supervisory control and data acquisition (SCADA) leader, instrumentation director, and head of operational technology being the most likely job roles to cover this function.

Utility owners or operators in small utilities are adding responsibility for cybersecurity to the long list of current duties for existing staff.

When looking at these titles by utility size, the picture becomes clearer. As noted previously, the workers at small utilities for a population of 10,000 or less take on numerous duties. Backing up that assertion, 40% of them indicated "other" for the title of the individual who handles cybersecurity responsibilities. Utility owners or operators in small utilities are adding cybersecurity responsibilities on top of other duties, meaning attention paid to cybersecurity issues is competing with other priorities.

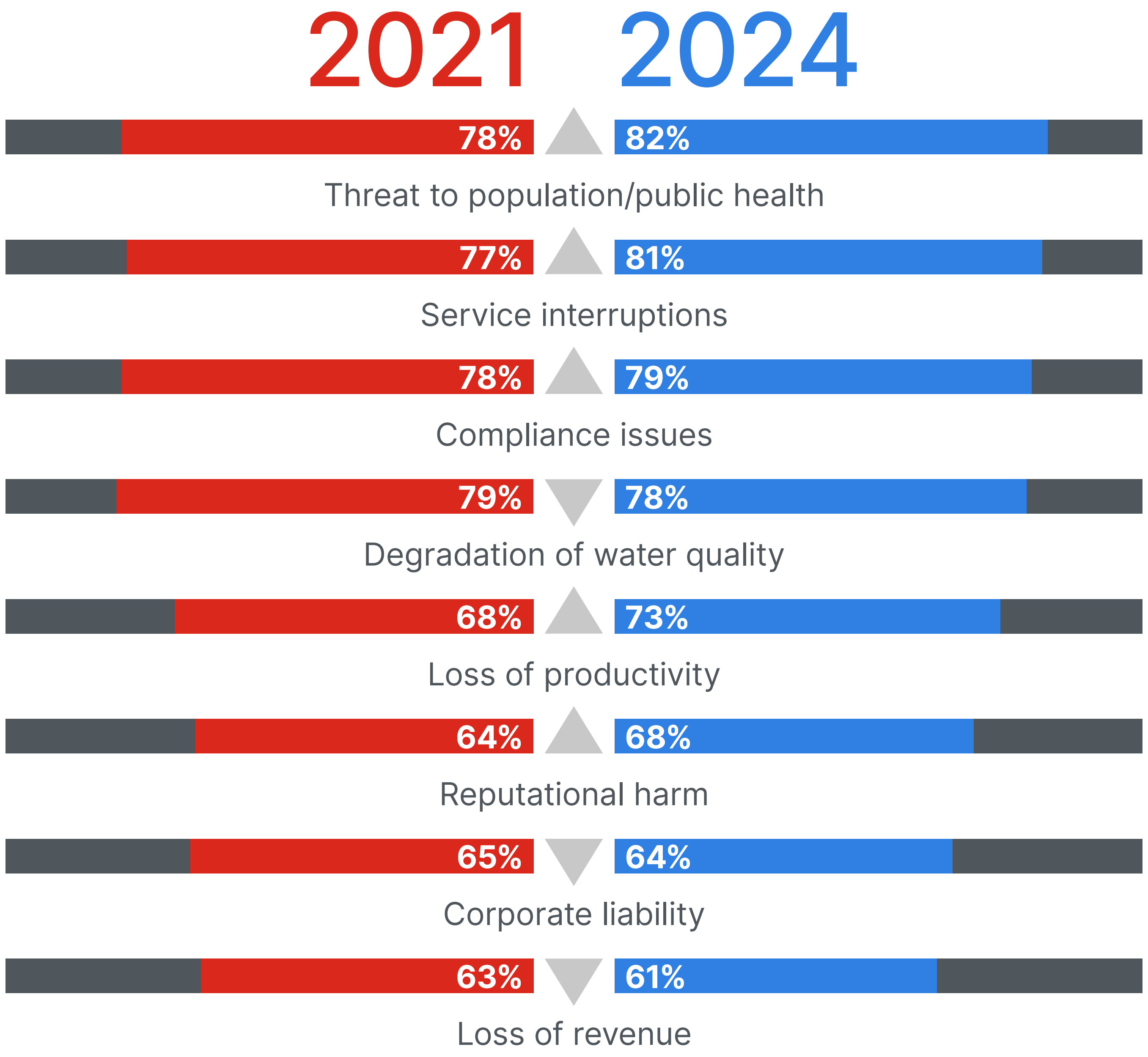
Addressing Looming Cyberthreats

Meanwhile, 80% of utilities with populations of 100,000 or greater have a staff member with a dedicated title to handle these issues. This shows a clear disparity in how active a utility can be with cybersecurity matters due to its size and the fact that small systems are more likely to struggle to meet cybersecurity goals.

The key areas of concern include threats to population/public health, service interruptions, and compliance.

The top cybersecurity concerns for 2024 were similar to those in 2021. As the potential cybersecurity threats continue to evolve and become increasingly sophisticated, the key areas of concern include threats to population/public health, service interruptions, and compliance issues. Other concerns include productivity losses, the potential for reputational harm, and corporate liability. (See Figure 4.)

Figure 4: When it comes to cybersecurity concerns, how important are the following to your agency or organization?



The top cybersecurity concerns for 2024 respondents were threat to population/public (82%), service interruptions (81%) and compliance issues (79%). The top challenges were similar to 2021 with degradation of water quality (79%) listed as the top concern in 2021.

Addressing Looming Cyberthreats

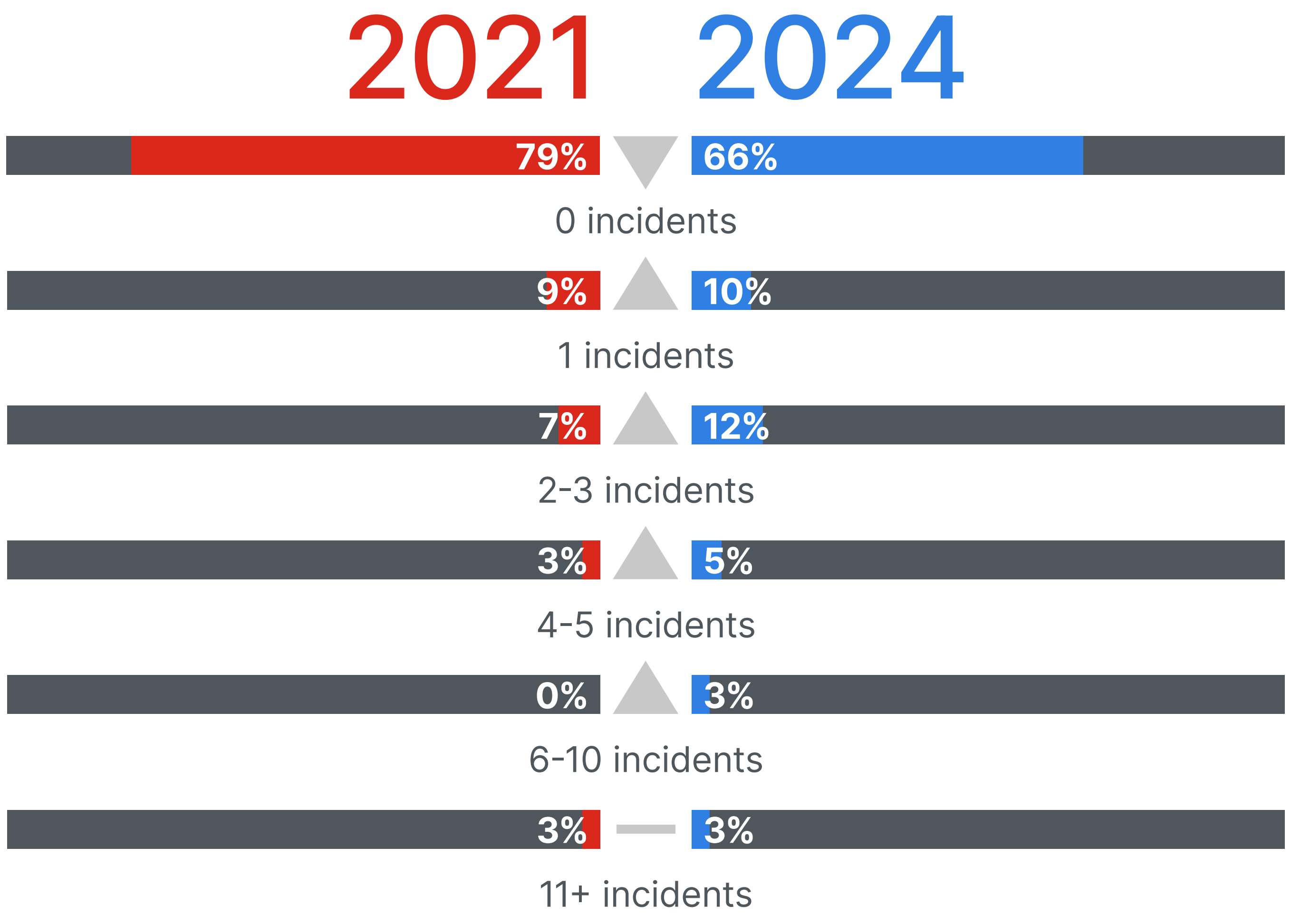
The types of cyberattacks that respondents are most concerned with were ransomware and malware/phishing, both of which were also key areas of concern in 2021. Right now, the top concerns are ransomware (65%), malware/phishing (63%), and physical attacks (23%). This concern for these utilities is warranted as they are maintaining similar, if not more sophisticated, records of their customers when compared to large retail chains like Target, which have suffered from ransomware attacks on their customer data. Ransomware can also spread to operational systems, taking SCADA offline and forcing on-site or manual operation while the organization recovers.

Compared to 2021's numbers, respondents are seeing more cyberattacks overall. (See Figure 5.) This shift aligns with the growing concern of cyber risk in water utilities and the growing prevalence of attacks on those water systems.

This year, 33% of survey respondents reported having at least one cyber incident over the last 12 months, compared to just 21% in 2021. The number of reported breaches was higher in every category compared to 2021.

Two-thirds of respondents (66%) said their organizations' exposure to cyberattacks is about the same as it was a year prior. Twenty-three percent say the potential security exposure threat has escalated (versus 26% in 2021). The smallest utilities (those with fewer than 10,000 customers) believe the threat has increased, while just 7% of the 100,000+ group report such concerns.

Figure 5: How many cyber incidents or IT/OT security related breaches has your agency or organization experienced in the last 12 months?



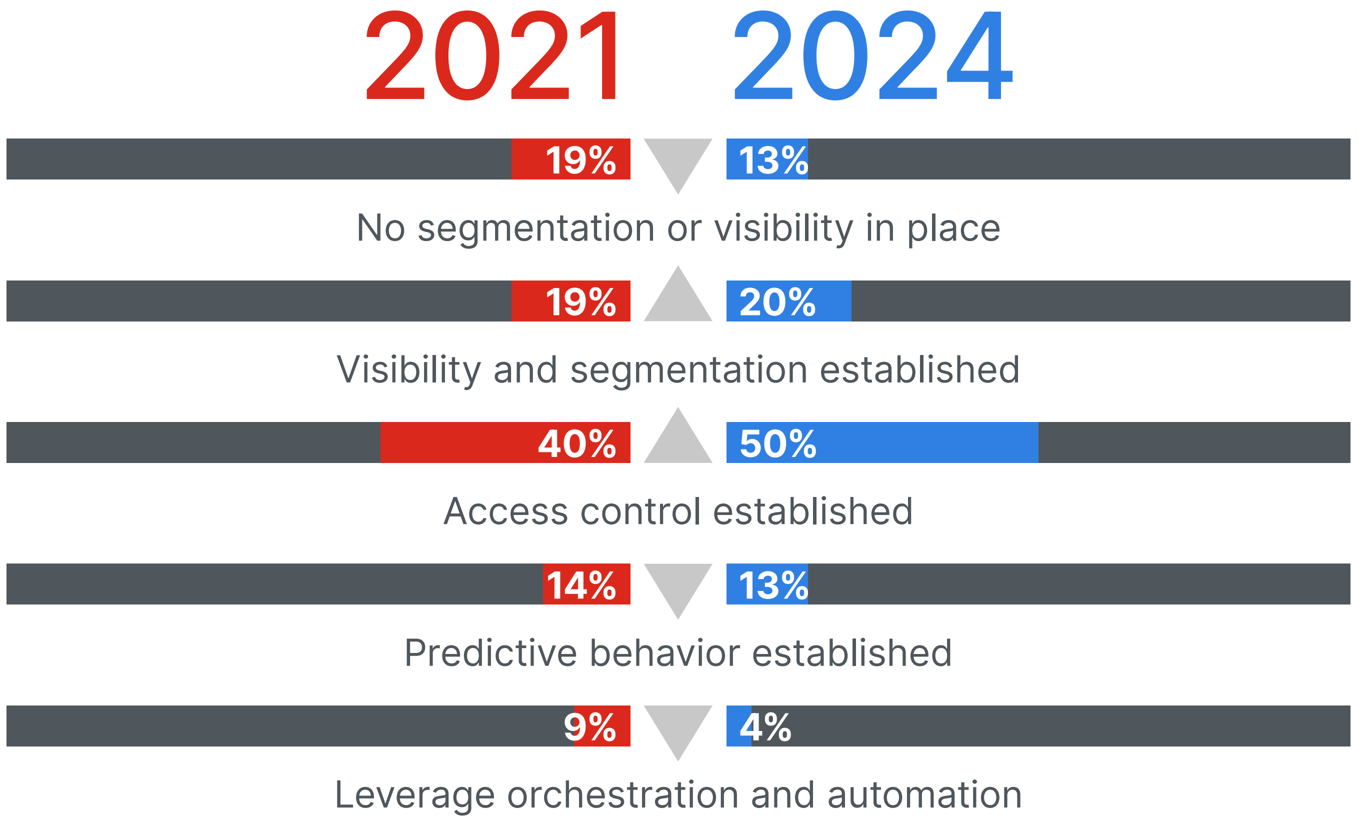
Compared to the numbers in 2021, respondents are seeing more cyberattacks overall, despite two-thirds (66%) reporting no attacks in the past 12 months. That percentage is down from 79% having no attacks in 2021.

It’s evident that water and wastewater utilities are slowly maturing and progressing in terms of their adoption of basic or initial cybersecurity measures.

Self-reported cyber maturity has increased over the last three years, perhaps due to the increase in attacks and perceived risks. When describing their organizations’ level of cybersecurity preparedness, most have established access control, while others are using visibility and segmentation, predictive behavior monitoring, or orchestration and automation. (See Figure 6.) Based on the survey, it’s evident that water and wastewater utilities are slowly maturing and progressing in terms of their adoption of basic or initial cybersecurity measures.

Respondents also indicated that they have more cybersecurity controls in place, with increases in every type of security control. Organizations also reported having more elements as part of their existing strategy, with the biggest jump in

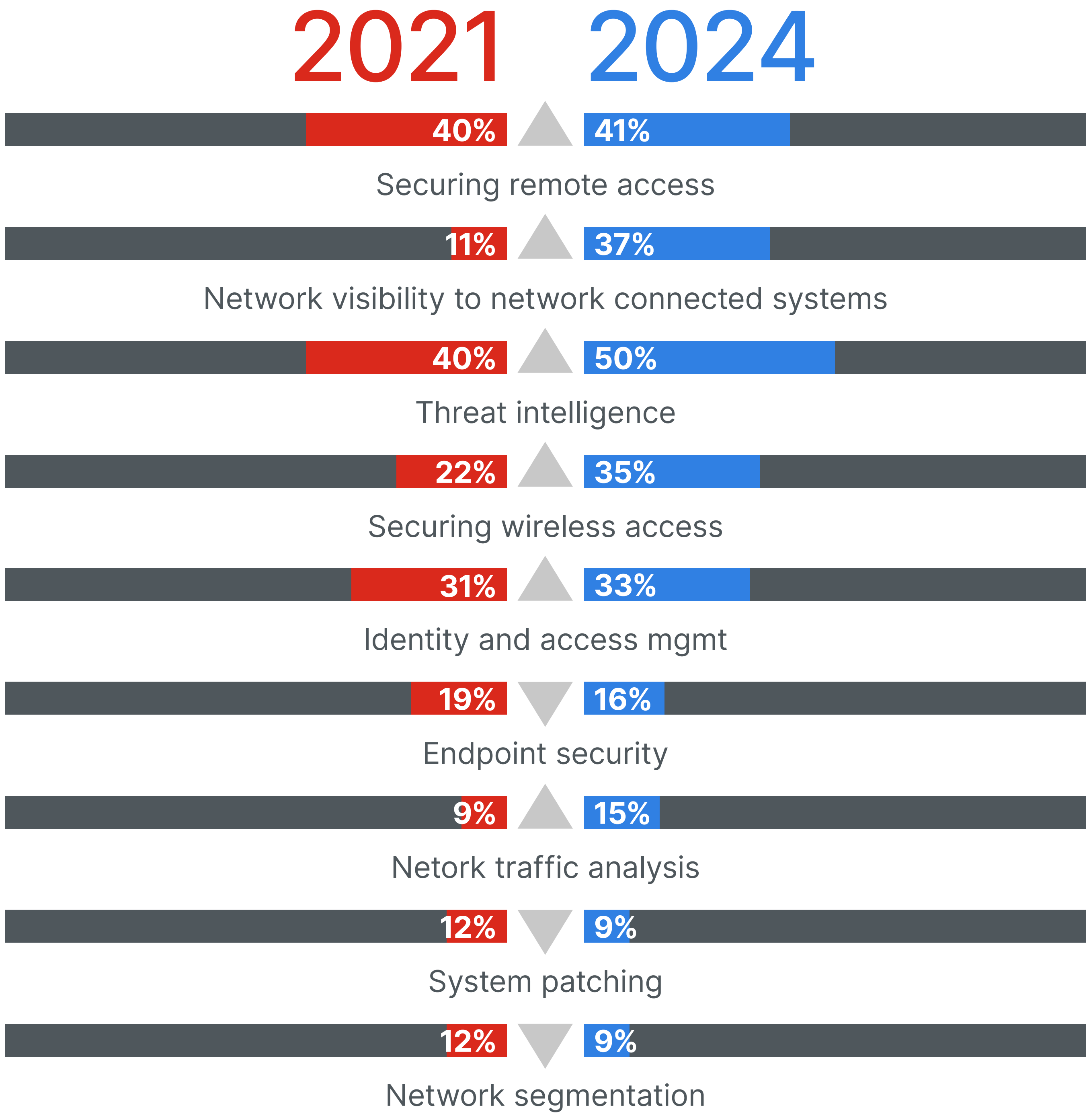
Figure 6: Which of the following statements best describes the maturity of your organization or agency’s cybersecurity preparedness?



Five in ten respondents (50%) said that their organization had access control established compared to 40% in 2021. 13% had predictive behavior.

Figure 7: Which of the areas are your organization or agency most focused on over the next 12 months to improve your cybersecurity preparedness?

The top areas that organizations are focusing on over the next 12 months were securing remote access (41%), network visibility to network-connected systems & assets (37%) and threat intelligence (35%).



network visibility (83% versus 69% previously). Organizations are planning to adopt a larger range of security controls than in our last survey, with securing remote access remaining a top priority.

The water sector has seen a significant jump in the adoption and prioritization of network visibility and the use of threat intelligence. This likely aligns with greater security maturity overall, awareness of best practices, and familiarity with operational technology (OT) security technologies.

To improve cybersecurity preparedness, organizations want to secure remote access, enhance network visibility into network-connected systems, improve threat intelligence, and secure their wireless access points. (See Figure 7.) The latter could include monitoring systems such as remote pumping stations or lift stations, wireless control signals for remote stations or systems within a plant's

Measuring Cybersecurity Maturity

campus, or cellular device signals from advanced metering infrastructure. Additional areas of investment include identity and access management, endpoint security, and network traffic analysis.

Most agencies (72%) say their agency's board of directors understands the value of a robust cybersecurity program, and an equal percentage say their board is far more concerned with cybersecurity than it was 12 months ago. (Chart not shown.) This is not surprising, considering data in this report shows a rise in reported cyberattacks and heightened awareness of cybersecurity due to the presidential administration's efforts to bolster cybersecurity for water systems. These factors, along with increasing media coverage of cyberattacks, likely contributed to the changes in boards' sentiments on cybersecurity.

Respondents spend the most time ensuring compliance, with 57% spending more than five hours a week and 25% spending more than 20 hours each week on this aspect of their jobs. (Chart not shown.)

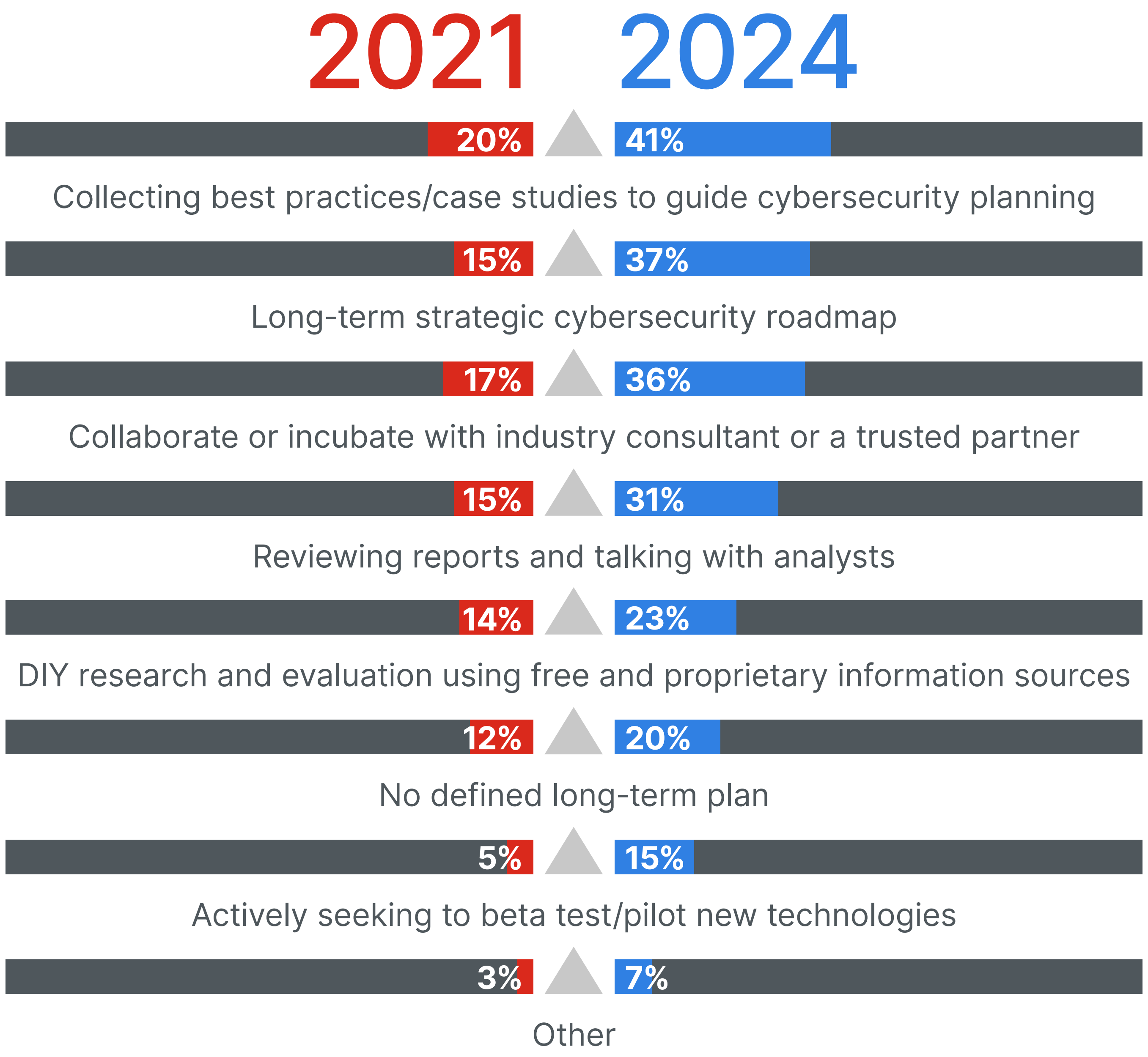
Getting Smarter

Water and wastewater utilities consult a broad range of sources to inform their cyber strategies, with the top sources being the collection of best practices and having long-term cyber roadmaps in place. This year's survey revealed a significant jump in the use of long-term roadmaps and nearly twice as many utilities actively piloting new security technologies. (See Figure 8.)

Compared to 2021, those with no plans to invest decreased or stayed the same in all areas of cybersecurity. In a broader sense, external communications efforts have risen drastically in the water market in the past two to three years, partially to explain the nuance of new regulations to customers, but also to raise awareness of cyber risks. The growing focus on public communications and crisis management is a huge paradigm shift for this market that, perhaps, grew comfortable being "the silent utility." That era is over.

Figure 8: Which of the following does your organization or agency use to make cybersecurity technology decisions?

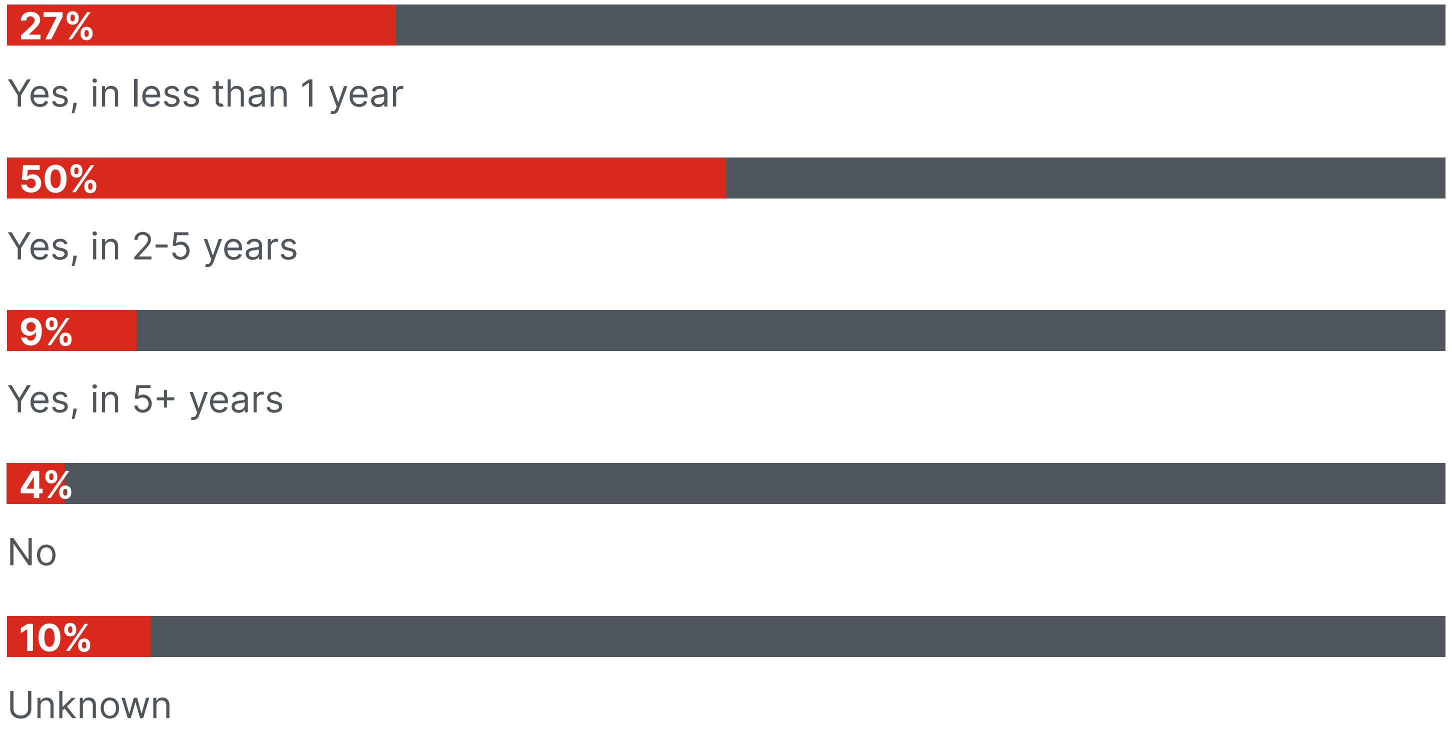
Three in ten respondents (31%) were collecting best practices/case studies to guide cybersecurity planning, followed by implementing long-term strategic cybersecurity roadmaps (27%) and collaborating and incubating with industry consultants or trusted partners (26%).



Getting Smarter

When asked about the top influences or impacts on their organizations going forward, the majority of respondents signaled that increased regulations and compliance would be major influences over the next one to five years. (See Figure 9.)

Figure 9: In your opinion, do you anticipate increased regulation and compliance will impact the water and wastewater utility?



Half of respondents (50%) felt that within the next two to five years there will be increased regulation and compliances that will impact water and wastewater utility.

Conclusion: America's Water Infrastructure Needs a Digital Force Field

As bad actors take advantage of newly disclosed vulnerabilities, water facilities need robust security scrutiny for their systems and network architectures. The threat landscape has changed for water utilities, which are now in the crosshairs of multiple threat actors, including cyber espionage (Volt Typhoon), cybercriminals (ransomware), hacktivists (cyber avengers), and state-aligned risks.[6] Utilities and agencies must maintain a strict patching regimen to reduce the risk of exploitation across all these threats.[7]

Proactive control system defense is required to preserve safety of operations.

The industrial control system (ICS) threat landscape continues to evolve, influenced by increased targeting of critical infrastructure — water and wastewater plants included. As these targeted threats against critical infrastructure and ransomware events continue to evolve, the message is clear: Proactive control system defense is required to preserve safety of operations.

What's more, a well-designed, ICS-specific, defense-in-depth security program is not a "nice-to-have" — it's essential.

Across all industries, 85% of leaders say their organizations have security awareness and training programs, yet more than 50% believe their employees still lack cybersecurity knowledge.[8] Because OT has been traditionally isolated, security has not been top of mind, thus basic security hygiene is not implemented within many OT environments. Safety and security must be systemic within an organization to help best practice adoption. OT security best practices include network segmentation, visibility to data, users and applications on the network, and secure remote access, which align to the most important cybersecurity controls to implement for an organizations, regardless of industrial sector.[9]

Securing the nation's water infrastructure isn't just about protecting treatment plants and pipes; it's about safeguarding public health and safety. By prioritizing cybersecurity, investing in technology, educating employees, taking inventory of assets, reducing potential attack surfaces, and taking action now, water and wastewater facilities can continue to ensure a reliable, safe resource for their communities.

[6] finance.yahoo.com/news/fortinet-threat-research-finds-cybercriminals-130000030.html
[7] Ibid.
[8] fortinet.com/content/dam/fortinet/assets/reports/report-2023-security-awareness-and-training.pdf
[9] sans.org/white-papers/ics-ot-cybersecurity-survey-2023s-challenges-tomorrows-defenses/experience-cyber-attacks-that-target-employees

About the Survey

The data for this report was collected via email April 4-19, 2024, by Endeavor Business Intelligence on behalf of Fortinet. The methodology conforms to accepted marketing research methods, practices, and procedures. Endeavor emailed invitations to participate in an online survey to members of its WaterWorld and Wastewater Digest databases. Endeavor received 350 usable responses and 230 completes. Each qualified respondent who completed the survey was given a $10 gift card.

The organizations respondents work for were varied compared to the data from 2021. A quarter of respondents work in water and wastewater systems and/or plants (25%) or local governments (22%). The majority (25%) are employed by water and wastewater systems (versus 34% in 2021), local government (22% versus 18%), consulting firms (11% versus 5%), and water-only systems and plants (9% versus 22%). Other respondents work for wastewater-only systems, equipment and supply manufacturers/distributors, and federal agencies.

Two-thirds of respondents' organizations (67%) were municipally owned and operated (versus 65% in 2021). The total population served was mixed, with 43% serving more than 25,000 people (compared with 49% in 2021) and 15% having over 500,000 customers (versus a previous 13%). Nine percent of respondents work for organizations with fewer than 500 associates (11% in 2021), and 27% are employed by groups with somewhere between 501 and 10,000 workers (versus 28% in 2021).

The top job roles for respondents were executive/administrative management (31%) and operations (23%). This job role distribution was similar in the 2021 survey.

Founded more than 20 years ago in Sunnyvale, California, Fortinet continues to be a driving force in the evolution of cybersecurity and the convergence of networking and security. Securing people, devices, and data everywhere is our mission. To that end, our portfolio of over 50 enterprise-grade products is the largest integrated offering available, delivering proven cybersecurity everywhere you need it. More than 755,000 customers trust Fortinet solutions, which are among the most deployed, patented, and validated in the industry. Learn more about Fortinet's OT Security Platform at **fortinet.com/OT**.