WaterWorld

Cybersecurity in Water Management Facilities

SPONSORED BY: FORTINET

Table of Contents

Executive Summary

Cyberattacks are a growing threat to water utilities. Recent incidents have garnered media attention as potential threats to water systems endanger public health and the environment.

Water systems epitomize volatile critical infrastructure and are designated in the National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems. This requires baseline and sector specific goals to detect and prevent cyber threats. In addition, America's Water Infrastructure Act includes mandates to improve the cybersecurity of water systems.

Fortinet surveyed water utility leaders during the fourth quarter of 2021 to understand utilities' status and future needs for improved water system cybersecurity.

Key Findings

1. Changing Technological Priorities

Past technological priorities for water utilities focused on meeting regulatory compliance, and 83% of respondents had confidence in this area. More recently, the focus has shifted toward improving system resilience and accommodating digital transformation. Increased connectivity leaves utilities more vulnerable to cyberattacks, increasing the need for improved cybersecurity. Only 49% of respondents felt confident in their cybersecurity technologies, and cybersecurity was the highest priority for future technology investment.

2. Responsibility for Cybersecurity

While 29% of respondents noted the Head of Information Technology (IT) managed their utility's cybersecurity, 30% chose "Other." Write-in responses spanned a wide range of positions, many of which would typically have no cybersecurity experience. Survey responses indicated that "someone else" was responsible for cybersecurity. Ultimately, all employees share some responsibility for cybersecurity.

3. Need for Situational Awareness

The consequences of a cyberattack on a water/wastewater system are extremely high. In addition to potential harm to public health and the environment, utilities are subject to regulatory penalties in the event of a breach. Survey responses to questions on cyberattack concerns, experiences, strategy, and preparedness show respondents lack awareness of a cyberattack's potential for grave harm. In a question about perceived changes in the number of cyberattacks over the last year, most respondents (62%) believed there was no change. Without detection methods, cyberattacks can be "invisible" until it's too late.

4. Cybersecurity Education Imperative

When rating cybersecurity strategy components, more than half the respondents reported Implementing/Improving Identity and Access Management was part of their strategy, followed by other cybersecurity strategies. However, 27% to 40% of respondents answered, "Don't Know." Similarly, respondents reported that the most significant challenge to improving their organizations' cybersecurity was a "poor understanding of what needs to change." These and other responses show the need for cybersecurity training to create a cybersecurity culture throughout the organization.

Introduction: Cybersecurity Threats to Water Utilities Are Increasing

Water utilities have continued to shift from isolated operational technology (OT) to a digitally connected infrastructure with information technology (IT) to obtain more accurate and time-sensitive/business-relevant data. While innovative technologies improve efficiency and effectiveness, they increase vulnerability to various cyberattacks.

Cybersecurity specific to water treatment systems in the United States gained the public's interest in recent years. Cybersecurity is an issue that attracted media attention, including news stories about potential security disasters in the water sector.

One of the most widely publicized breaches involved a small utility in Oldsmar, Florida. A bad actor hacked into water plant controls and raised the sodium hydroxide dosage setting to a toxic level. The on-site water plant operator quickly noticed the issue and averted the problem.

Other such incidents have occurred, often with little publicity. Examples include a January 2021 hack into a San Francisco Bay Area water plant that deleted water treatment programs. In October 2021, a former employee pleaded guilty to tampering with the computer system at a drinking water treatment facility in Ellsworth County, Kansas, shutting down the plant. Other issues include security breaches that targeted billing systems and an increase in ransomware attacks.

The White House is preparing a plan to help water utilities improve their ability to protect water systems from cyberattacks with the help of the Environmental Protection Agency (EPA) and Cybersecurity and Infrastructure Security Agency (CISA).

Cyberattacks have the potential to damage critical water infrastructure or contaminate water supplies, endangering public health and the environment. In addition, security breaches put customer data at risk, and ransomware can paralyze business activities.

To facilitate water/wastewater facilities gaining a stronger appreciation for cybersecurity awareness and needs, Fortinet prepared this report based on an online survey and research initiative. The survey targeted water utility leaders from the WaterWorld database. The most common responders included executive management, operations management, and engineering staff from municipally owned water and wastewater systems. These systems served a wide variety of population from less than 3,300 to over 100,000 people.

The report features data reflecting respondents' perspective on their utility's:

- Current and projected technologies
- Cybersecurity responsibilities, concerns and preparedness
- Future cybersecurity strategies, challenges and timeframes
- Self-assessment of cybersecurity posture

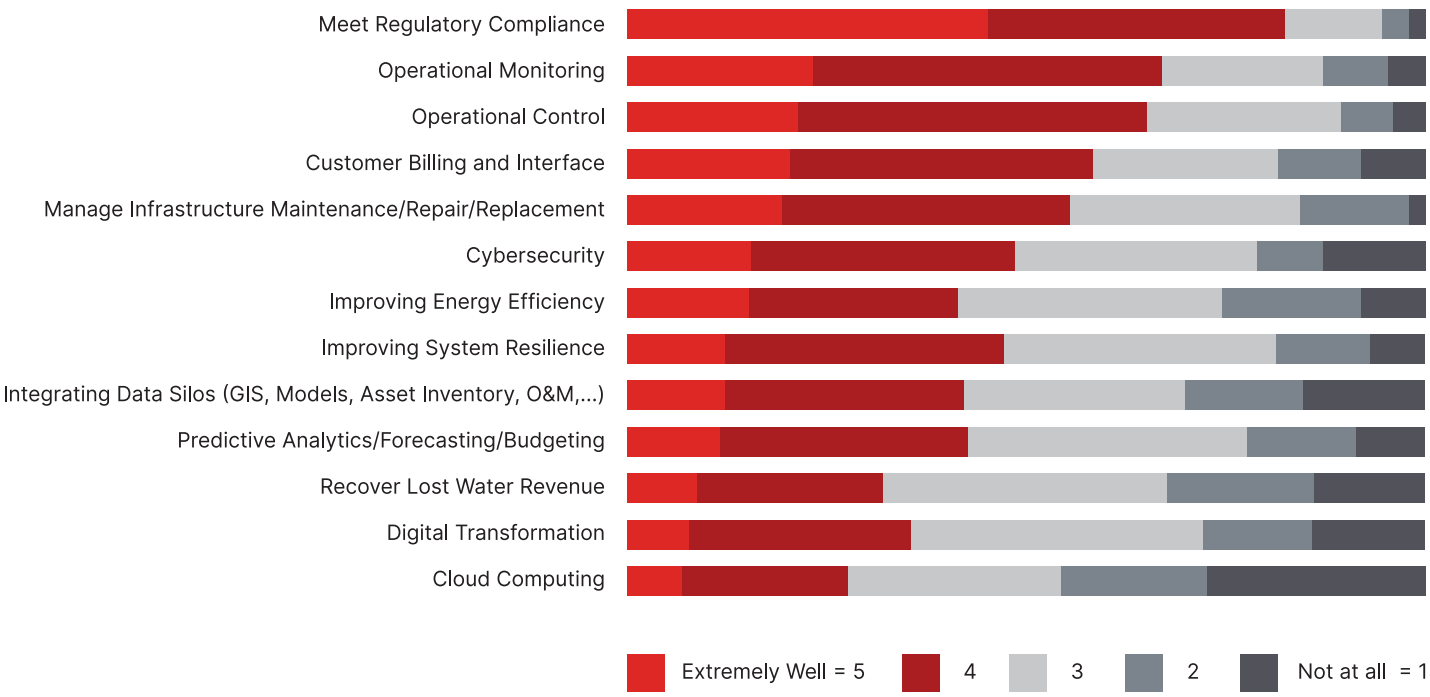
Water Utilities' Current and Predicted Technologies

Current Technologies Focus on Regulatory Compliance

Water leaders had the most confidence in technology used to support compliance with regulations (83%), along with operational monitoring and control. Utility billing and customer interface rank slightly below, as does asset management.

Confidence in their ability to meet cybersecurity needs ranks in the middle (49%), followed by sustainability and resilience tools. Newer technologies for integrating data silos, revenue recovery, predictive analytics, digital transformation and cloud computing were lowest on the confidence scale. However, cybersecurity becomes more crucial as these newer technologies are implemented.

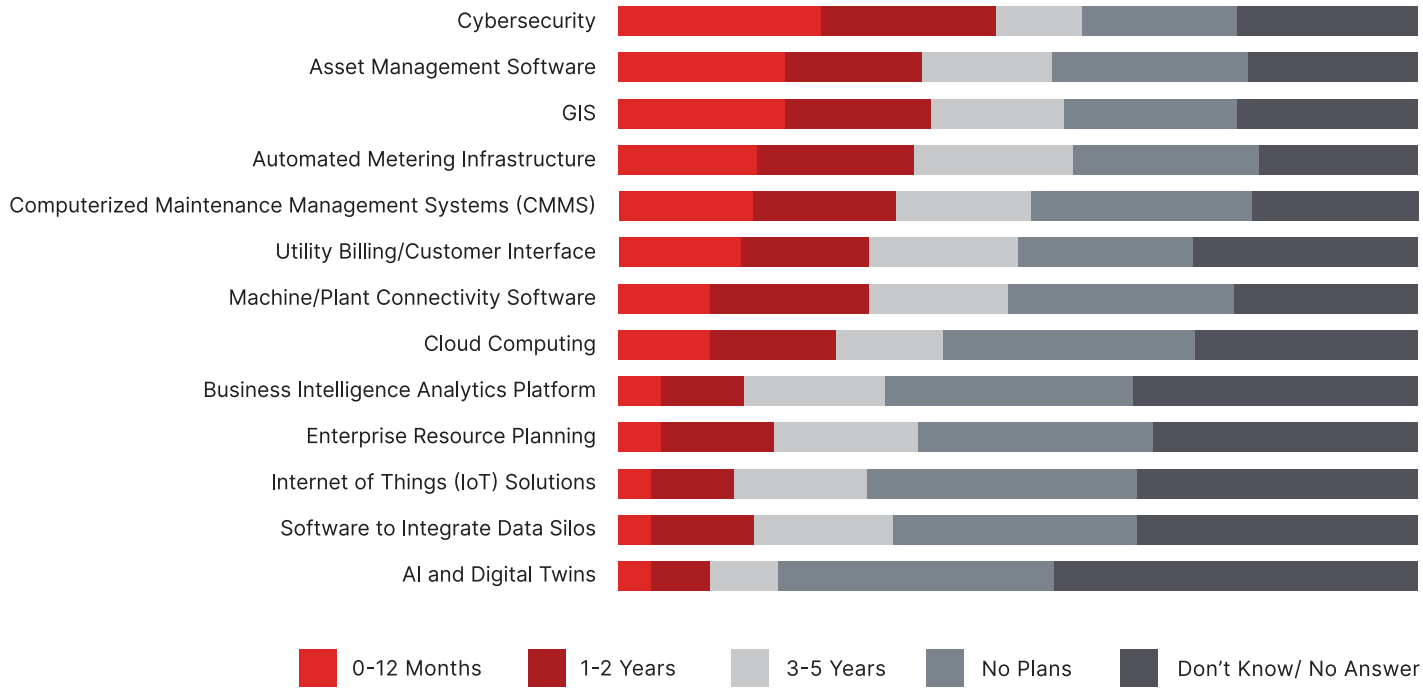
On a scale of 1 to 5, rate how well your current technologies support your organization or agency's ability to meet the following strategic or operational needs. (n varies from 239 to 249)



Utility Leaders Rank Cybersecurity as a Top Priority for Future Investment

Cybersecurity received the highest ranking for forecasted technology investment, with 26% of respondents planning for improvements in the next 12 months and 22% within the next 2 years. Slightly below were investments for asset management, Geographic Information Systems (GIS) and automated metering infrastructure.

In which areas of technology does your agency/organization plan to invest or improve over the following timeframes? (n varies from 220 to 224)

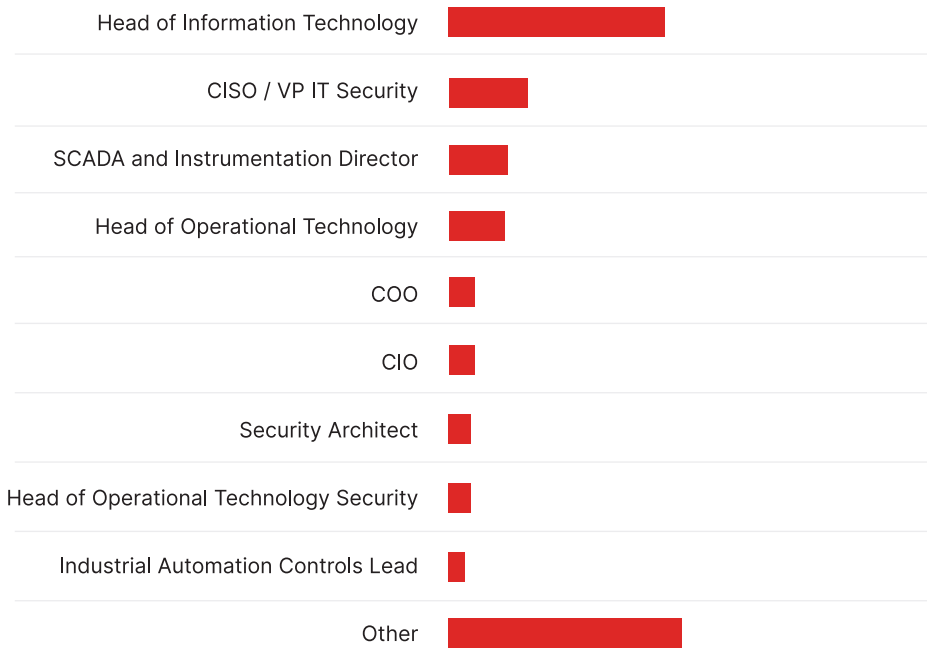


Cybersecurity Responsibilities, Concerns, and Preparedness

Responsibility for Cybersecurity Is Poorly Defined at Many Utilities

Per 40% of respondents, the Head of IT or the Chief Information Security Officer (CISO) were charged with managing cybersecurity. However, 32% of utility leaders reported "Other" persons had that responsibility. These included City Manager, Operator, Governing Board and Secretary, Mayor, Town Council, Human Resources and Finance Director. In most instances, such designation translates into an unlikely level of expertise in cybersecurity and doubtful leadership capacity to take appropriate and timely actions to protect the system. Given the critical nature of water utilities, overall responsibility for cybersecurity must be clearly defined.

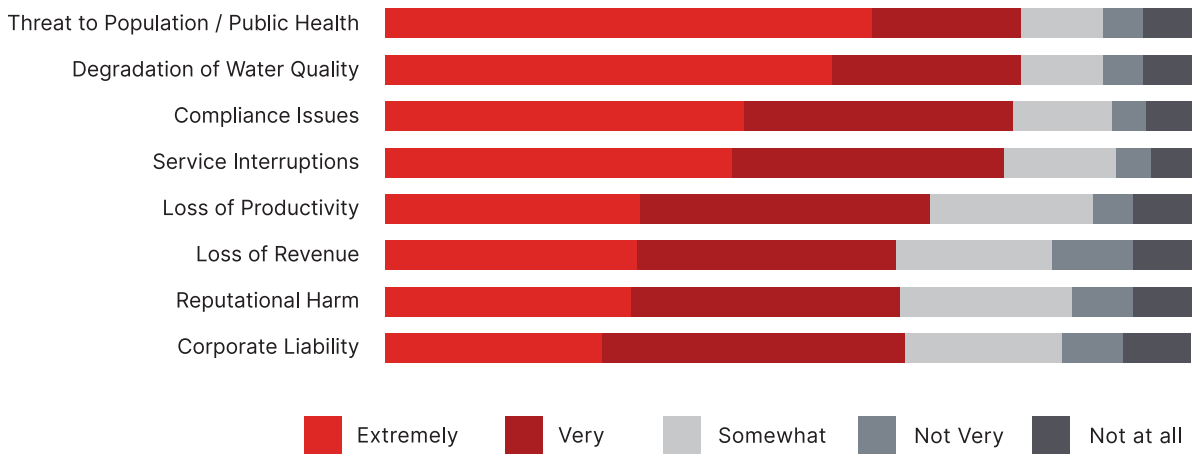
Who has overall responsibility for cybersecurity at your organization or agency?



Threats to Public Health and Water Quality Are Top Cybersecurity Concerns

When it comes to cybersecurity, water leaders are most concerned with threats to the population regarding public health and water quality degradation, with 79% of respondents ranking these concerns as extremely or very important. Closely following were compliance issues (78%) and service interruptions (77%).

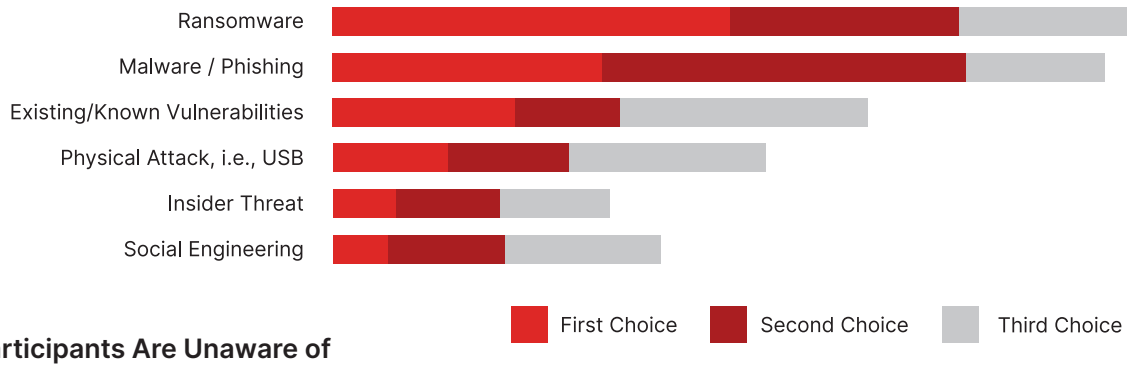
When it comes to cybersecurity concerns, how important are the following to your agency or organization? (n varies from 206 to 211)



More Concern About Malware Than Existing Vulnerabilities and Insider Threats

When asked about the type of cyberattack that garnered the greatest concern, study participants identified ransomware (37%) and malware/phishing (25%) as top worries. This is surprising, as the most publicized cyberattacks on water systems have been related to existing vulnerabilities and insider threats.

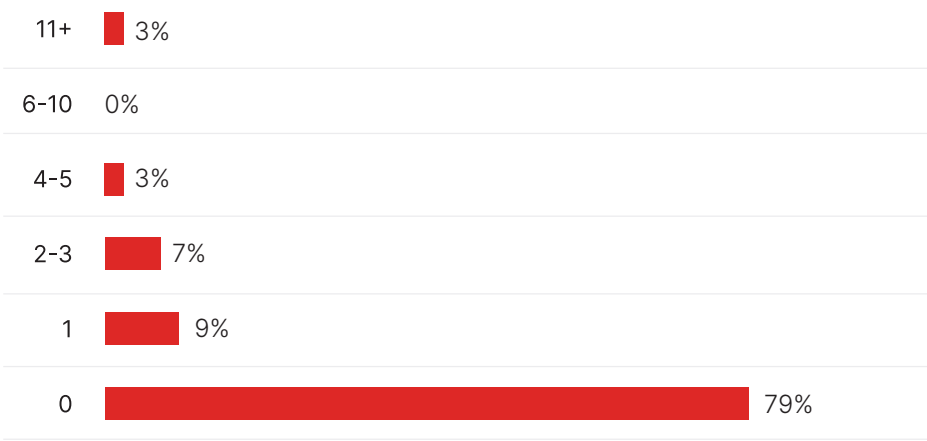
Please rank the level of concern of agency or organization for the following types of cyberattacks. (n = 189)

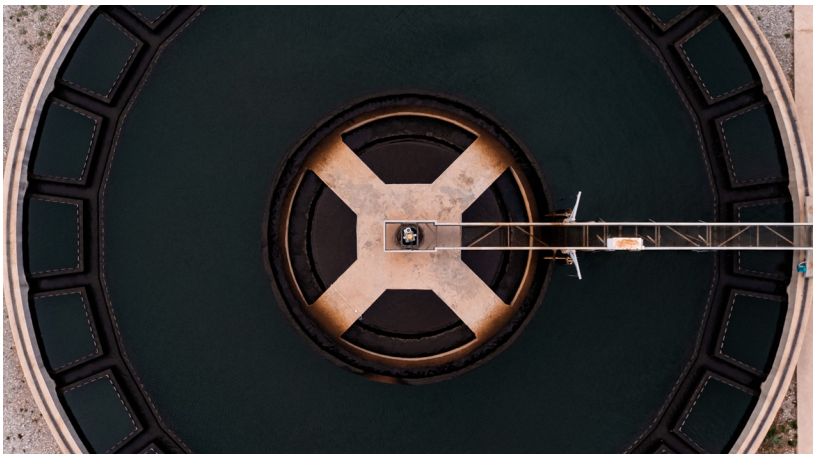


Survey Participants Are Unaware of Cyberattacks

The overwhelming majority (79%) of respondents indicated that their organization had no cyber incidents within the last 12 months. Conversely, a very small minority (3%) of participants offered they had experienced over 11 cyberattack experiences. The substantial number of participants reporting no cyberattacks might suggest that the water industry is extremely safe from these intrusions. The more likely takeaway is that water industry leaders may have a false sense of security. That would suggest that survey participants are simply unaware of the malicious activity surrounding their OT systems. Without intrusion detection, incidents and security breaches may occur, and hackers may be discovering vulnerabilities and ultimately gaining access without being noticed.

How many cyber incidents or IT/OT security related breaches has your agency or organization experienced within the last 12 months? (n = 197)



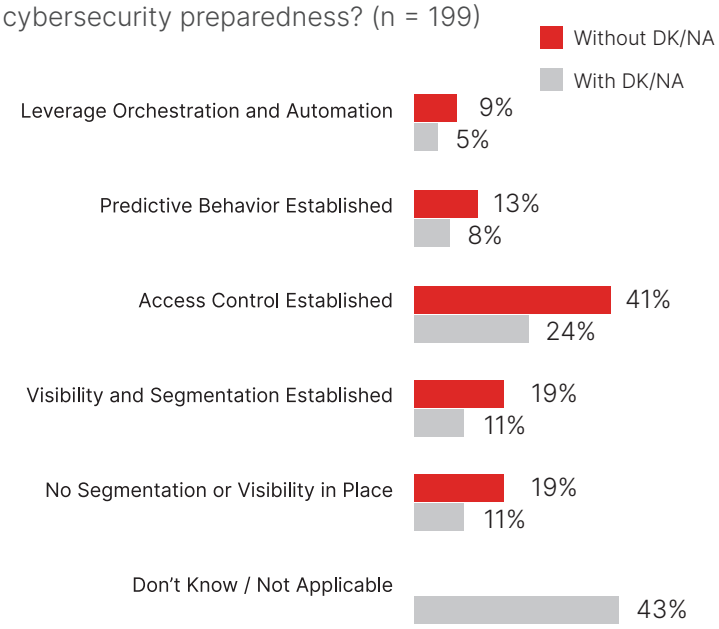


Cybersecurity Preparedness Needs Improvement

Of the survey participants that could comment knowledgeably, 41% said they had a maturity level of "Access control established." Only 9% were at a maturity level of "Leverage orchestration and automation." Choosing "Visibility and segmentation established" were 19% of respondents. And 19% of respondents reported "No visibility or segmentation established."

Most concerning was the fact that 43% of participants responded "Don't Know/Not Applicable" when describing their organization's cybersecurity preparedness level. This likely suggests that many water/wastewater facilities have yet to perform any type of self-assessment related to cybersecurity. What utility leaders "don't know" could have extreme consequences.

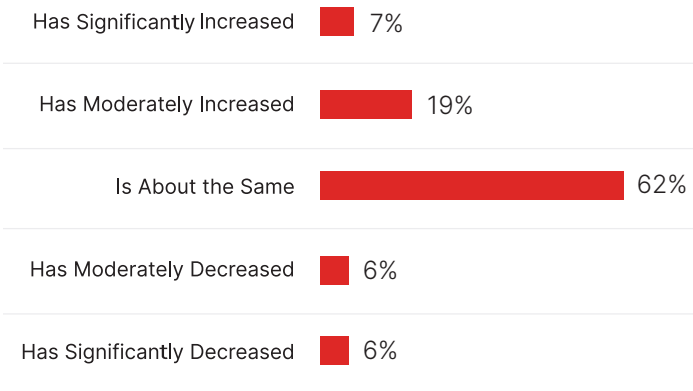
Which of the following statements best describes the maturity of your organization or agency's cybersecurity preparedness? (n = 199)



Perceived Change in Exposure to Cyberattacks Is Underestimated

More than 6 out of 10 (62%) of survey participants believe their potential exposure to cyberattacks has remained the same over the last 12 months, while 26% felt their exposure had moderately or significantly increased. Surprisingly, 12% of respondents believed their exposure decreased either moderately or significantly. Survey participants may have too much confidence in the integrity of their respective OT environment or, worse, be unaware of the level of cybersecurity threats. The potential for cyberattacks in every OT industry has increased exponentially, and the pandemic-driven necessity for more employees to accomplish work via digital connectivity has simply exacerbated the situation.

Over the last 12 months, the potential security exposure to cyberattacks on my agency or organization: (n = 196)



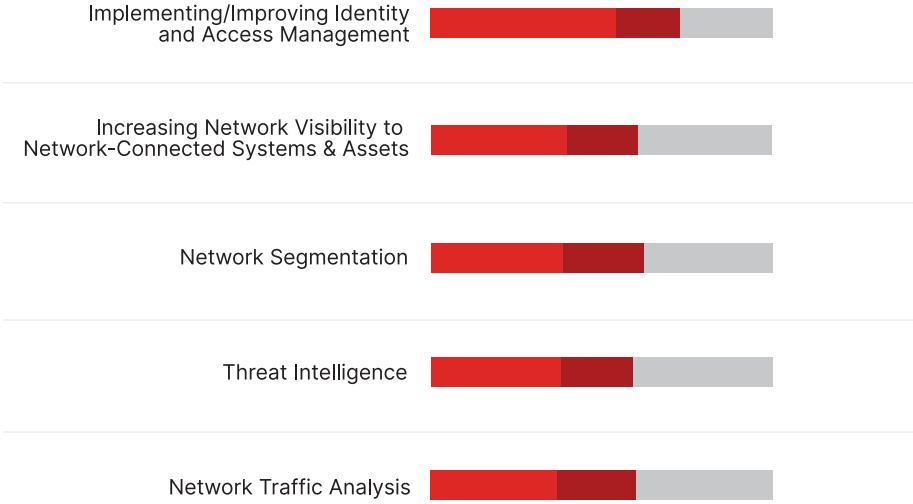
Cybersecurity Strategy

Cybersecurity Strategy Knowledge Gap

When probed regarding which components were part of their organization's cybersecurity strategy, over half (54%) of respondents reported "Implementing/Improving Identity and Access Management." All other measures were included in the strategies for 37% to 40% of the survey participants.

Twenty-seven percent to 40% of participants did not know what strategies were included in their cybersecurity plan. This amplifies a dire need for cybersecurity training and education for water industry leaders.

Which of the areas does your organization or agency have in place as part of your cybersecurity strategy? (n varies from 189 to 191)

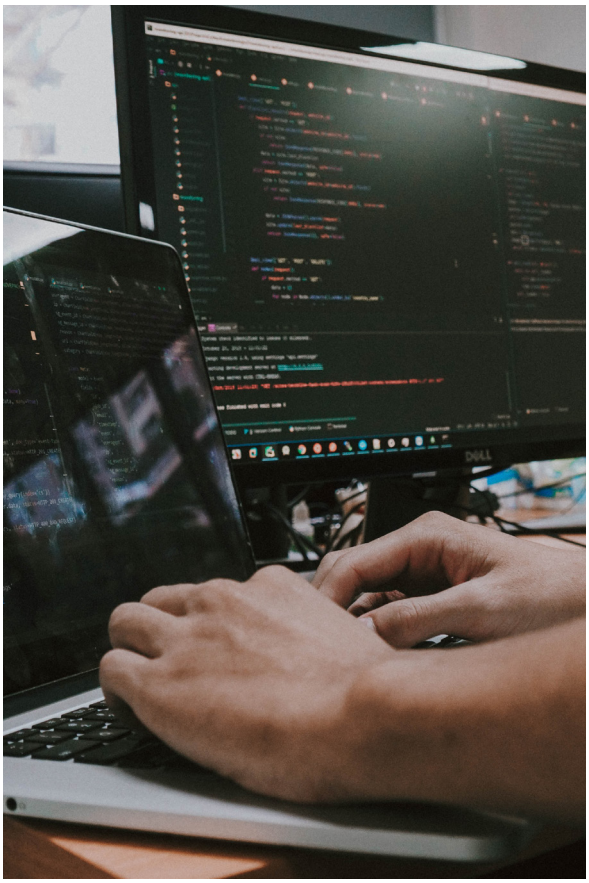


Variety of Sources Used for Making Cybersecurity Decisions

When making decisions about cybersecurity technology, almost one-third (31%) of survey participants relied upon industry consultants, while another 24% collected best practices/case studies, and 21% collaborated with a trusted partner. 18% of respondents conducted "do-it-yourself" research by reviewing reports or conversing with analysts. Another 18% pointed to their long-term cybersecurity strategy, while 14% reported they had no long-term strategy.

For most water systems, a "do-it-yourself" approach to cybersecurity is inadequate. Cybervillains are savvy in gaining access and employing sophisticated tactics and techniques. The high level of vulnerability and risk for water utilities demands competent sources to improve cybersecurity preparedness.

The 25% of respondents who had no answer or shared they did not know what sources were used for decision-making demonstrates the need for comprehensive training programs to implement an overall cybersecurity culture.



Which of these areas are your organization or agency most focused on over the next 12 months to improve your cybersecurity preparedness? (n = 177)
Up to 3 answers allowed.

Securing Remote Access	**41%**
Enforce Identity and Access Management	**31%**
Securing Wireless Access	**29%**
Implementing/Improving identity and access management	**28%**
Threat Intelligence	**21%**
Endpoint Security	**19%**
System Patching	**12%**
Network Segmentation	**12%**
Increasing Network Visibility to Network-Connected Systems & Assets	**11%**
Network Traffic Analysis	**9%**
Other	**12%**

Which of the following does your organization or agency use to make cybersecurity technology decisions? (n = 177) Multiple answers allowed.

Challenges to Cybersecurity System Improvement

When queried on challenges participants face to improving their cybersecurity, 35% of respondents said the most significant issue was a poor understanding of what needs to change. Inadequate funding sources was also a challenge for 32% of the study participants. Thirty percent of respondents noted lack of a clearly defined cybersecurity strategy was inhibiting improvement. Too much focus on running current operations was a factor for 29% of participants.

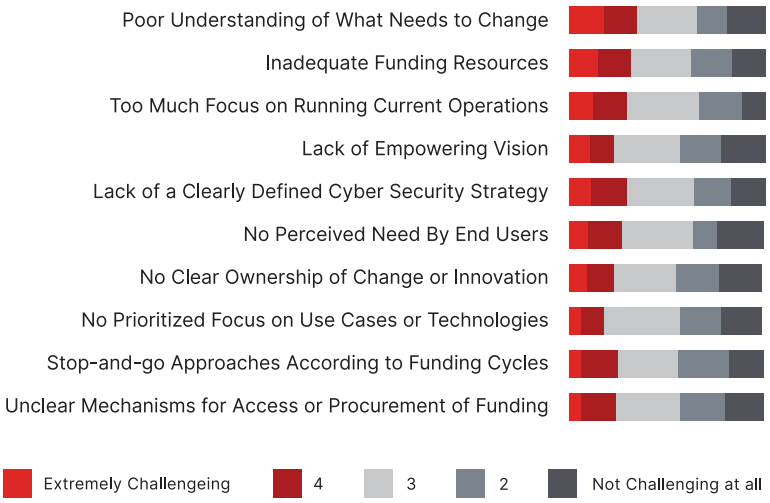
Once again, the high number of respondents who simply don't know what is needed emphasizes the inadequacy of cybersecurity education and training. Lack of funding and the fact that there's too much emphasis on running current operations also confirms that cybersecurity is not a top priority.

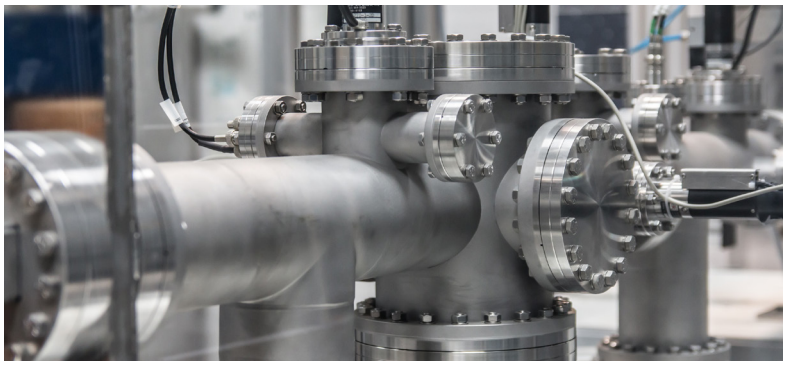
The Need for Investment in Cybersecurity

Investment timeframes for cybersecurity suggest that cybersecurity is lower on the priority list than expected given the heightened risk. Forty-four percent of respondents reported they would invest in network/asset protection within a short (0 to 12 months) to medium (1 to 2 years) timeframe. Incident detection was next on the list with 44% of participants planning to invest, followed by incident recovery with 43%. However, 18% to 26% of respondents had no plans to invest in cybersecurity at all, and 32% to 40% did not know about investment timeframes.

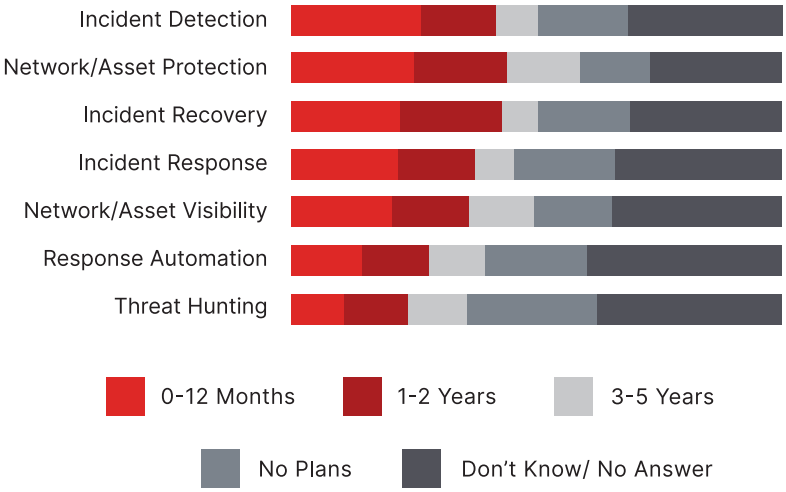
There is an immediate need for cybersecurity readiness and proactive defense strategy in the water sector, and prioritizing investment in cybersecurity is an imperative.

Which of the following are challenges to your organization or agency's progress when it comes to improving your cybersecurity technologies and systems? (n varies from 154 to 157)





In which areas of cybersecurity does your organization/agency plan to invest or improve over the following timeframes? (n varies from 151 to 155)

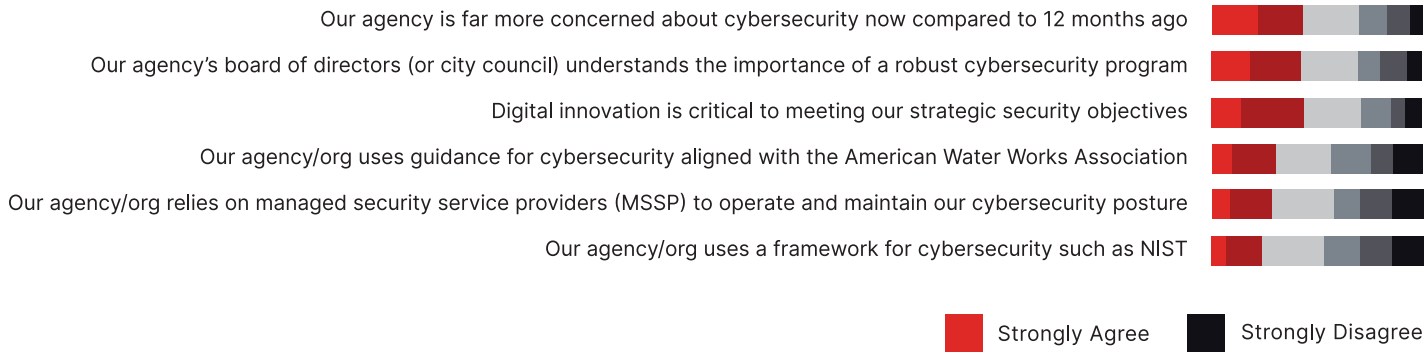


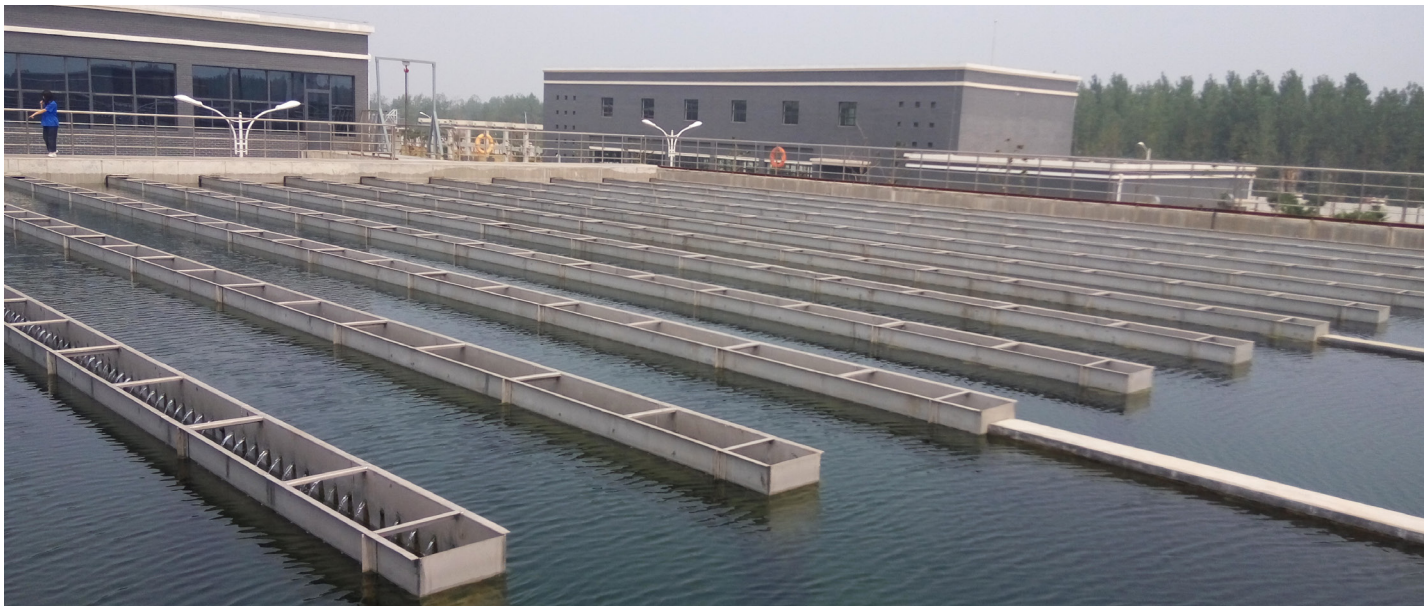
Cybersecurity Self-Assessment

Seventy-one percent of survey participants agreed that the industry and their respective companies are far more concerned about cybersecurity now than they were a year ago. Most respondents (71%) shared that digital innovation was critical to strategic security objectives and agreed that their board of directors understood the importance of a robust cybersecurity program (69%).

With added education, training and funding, water leaders can participate more fully to ensure their systems implement the necessary cybersecurity improvements.

To what extent do you agree or disagree with the following statements about cybersecurity and your agency or organization? (n varies from 151 to 158)





Conclusion

For almost the entirety of industrial history, OT for water/wastewater utility technology was isolated from IT. As technologies advanced, more systems transitioned to a digitally connected model where OT and IT integration is common. With the expansion of the attack surface due to the advent of smart meters, rapid growth in sensors and automation, predictive analytics, digital twins, and the Industrial Internet of Things (IIoT), cybersecurity must be a top priority.

This study highlights major gaps in cybersecurity education, training, and the creation of a cybersecurity culture. Water utility leaders are aware of the critical nature of their systems, yet not as aware of the risk posed by inadequate cybersecurity nor their abiding responsibility for that risk.

Funding is clearly an issue. Per the Cybersecurity Self-Assessment, most respondents felt their board of directors understood the importance of cybersecurity. If so, a proportional cybersecurity budget should be easy to justify. Placing a higher priority on cybersecurity to include a long-term strategy and adequate funding is critical to the protection of our water systems.

About the Research

Methodology, data collection and analysis were conducted by Endeavor Business Media on behalf of Fortinet. The survey was conducted from November 18 through December 6, 2021. Endeavor Business Media emailed invitations to take part in an online survey to members of the WaterWorld database. By December 6, 2021, Endeavor Business Media received 314 completed, qualified surveys.

Survey Participants

Survey participants included an excellent mix of Executive/Administrative Management (30%), Operations (28%) and Engineering and Operations Management (20%).

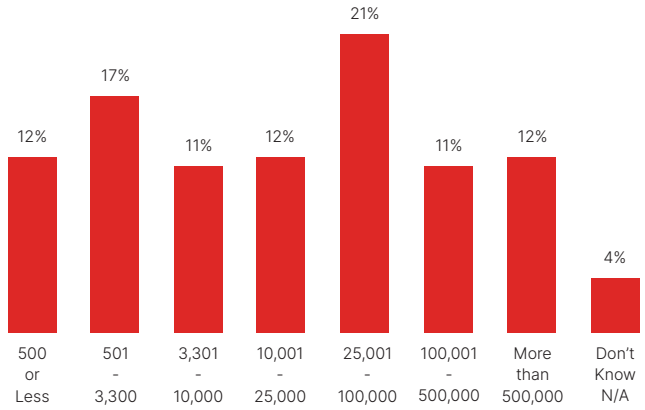
Organization/Agency Profile

Water and Wastewater, Water or Wastewater Only. Local Government comprised 18% of respondents and 65% of respondents worked for a Municipally Owned Organization or Agency.

Population Size Served

A wide variety of population sizes were represented.

What is the total population served by your agency or organization? (n = 282)



For more information on how to improve cybersecurity for your utility, visit fortinet.com/OT or email OT@fortinet.com.