WATER AND WASTEWATER SYSTEMS

CYBERSECURITY

2021 STATE OF THE SECTOR

Water Sector Coordinating Council

NAWC National Association of Water Companies · American Water Works Association · Association of Metropolitan Water Agencies · Water Environment Federation the water quality people · NACWA · NRWA · WATER ISAC · The Water Research Foundation

JUNE 2021

CONTENTS

Executive Summary

With threats from increasingly sophisticated and destructive attackers, cybersecurity has become a top priority for water and wastewater systems. Recent incidents have added urgency to discussions within the sector and with Congress and in federal agencies on how best to help utilities improve their cybersecurity.

To help guide discussions with policymakers and to inform the sector's own cybersecurity programs, the Water Sector Coordinating Council (WSCC) - an advisory body comprising the national water and wastewater associations, the sector's research foundation and WaterISAC - collaborated on a utility survey to develop a picture of current cybersecurity practices in the sector to better articulate the challenges and needs of the sector.

This voluntary survey was distributed to utilities across the country by the nation's water and wastewater associations. The results represent a first-of-its-kind snapshot of the Water and Wastewater Systems Sector cybersecurity posture.

The survey, conducted in April 2021, resulted in 606 responses from water and wastewater utilities. The results show a range of cybersecurity preparedness levels across the sector, with many excelling in their efforts with current resources but with others demonstrating room for improvement and a need for greater support.

Water Sector Coordinating Council

Member Organizations

- American Water Works Association
- Association of Metropolitan Water Agencies
- National Association of Water Companies
- National Association of Clean Water Agencies
- National Rural Water Association
- Water Environment Federation
- Water Information Sharing and Analysis Center
- The Water Research Foundation

The Water Sector Coordinating Council is a policy, strategy and coordination mechanism for the sector in interactions with the government and other sectors on critical infrastructure security and resilience issues.

Challenges

Like all sectors, water and wastewater systems are targets, directly or indirectly, of cyber attackers, but complicating any set of solutions is the demographics of the sector. There are approximately 52,000 community water systems and approximately 16,000 wastewater systems in the United States.

Among these utilities are a wide range of capabilities and capacities for cybersecurity enhancement. Many are subject to economic disadvantages typical of rural and urban communities. Others do not have access to a cybersecurity workforce. Operating in the background is that these utilities are struggling to maintain and replace infrastructure, maintain revenues while addressing issues of affordability, and comply with safe and clean water regulations.

Needs

Survey respondents identified several needs to help them improve cybersecurity.

The top four categories are:

- Training and education specific to the water sector,
- Technical assistance, assessments, and tools,
- Cybersecurity threat information, and
- Federal loans and grants.

With the exception of federal loans and grants, many such resources already exist between those developed by the sector itself and those contributed by federal agencies. But clearly there is a need for additional resources in order to reach a greater audience among our large and diverse sector. The development and promotion of these resources will require a combined effort between the sector, government agencies, and partners.

Further, nearly 30% indicated a need for information technology (IT) and operational technology (OT) supply chain integrity, which demands strong federal leadership.

Respondents by Job Type

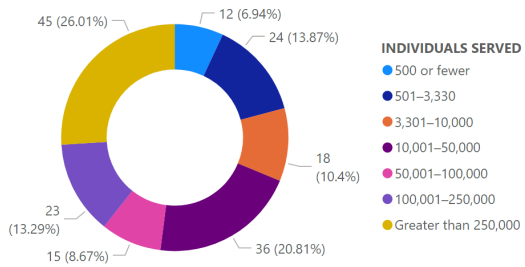
ANSWER CHOICES	RESPONSES	
CIO, CTO, CFO	9.76%	48
CISO, Sr. Security Analyst, System Administrator	7.93%	39
IT Manager, IT Specialist	14.84%	73
Other Executive Management or Board Member	28.46%	140
Water Engineer, Operations Director	39.02%	192
TOTAL		492

Cybersecurity Needs in the Sector

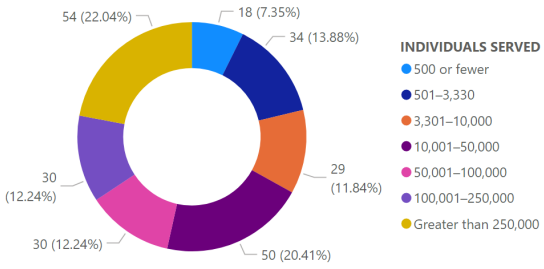
The following sector needs were identified by respondents. Further breakdown of needs by utility size are provided in the charts below.

ANSWER CHOICES	RESPONSES	
Technical assistance, advice, assessments or other support	47.47%	282
Federal grants or loans for cybersecurity equipment or services	41.08%	244
Training and education targeting the water sector	51.01%	303
Assurance of supply chain integrity for IT and OT hardware and software	29.12%	173
Funding to hire cybersecurity personnel	29.80%	177
Cybersecurity threat information	41.25%	245
I'm not sure	17.68%	105
No assistance is needed	12.46%	74
Total Respondents: 594		

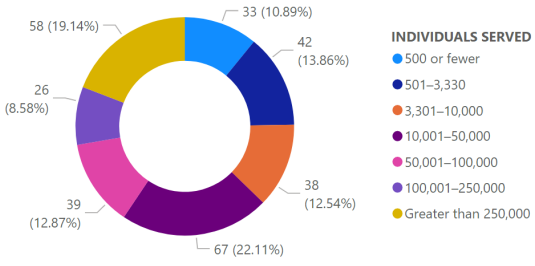
Count of NEED Assurance of supply chain integrity for IT and OT hardware and software by INDIVIDUALS SERVED



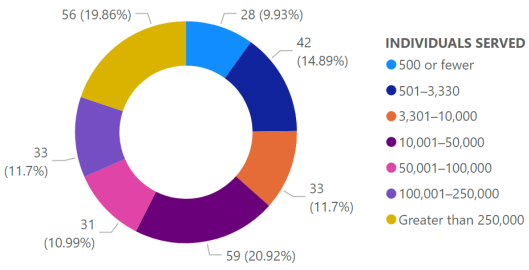
Count of NEED Cybersecurity threat information by INDIVIDUALS SERVED



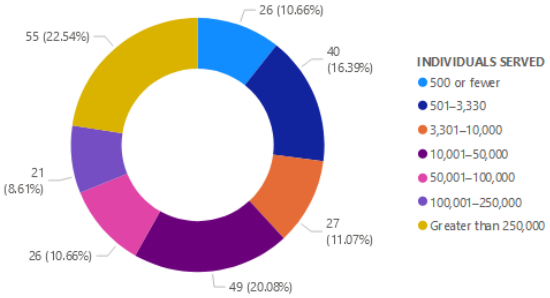
Count of NEED Training and education targeting the water sector by INDIVIDUALS SERVED



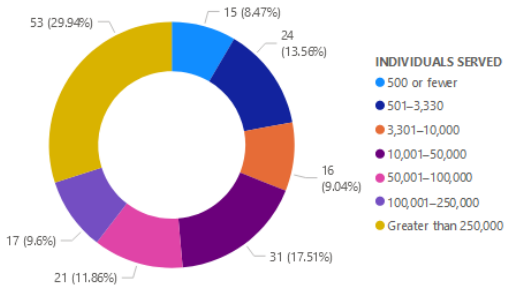
Count of NEED Technical assistance, advice, assessments or other support by INDIVIDUALS SERVED



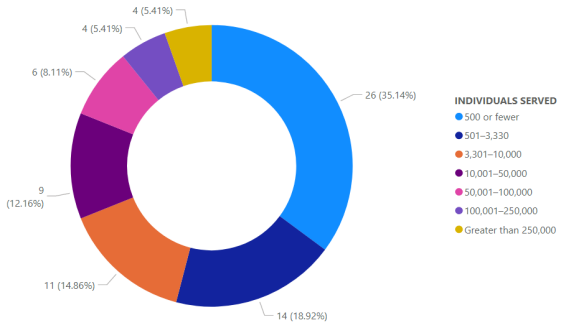
Count of NEED Federal grants or loans for cybersecurity equipment or services by INDIVIDUALS SERVED



Count of NEED Funding to hire cybersecurity personnel by INDIVIDUALS SERVED



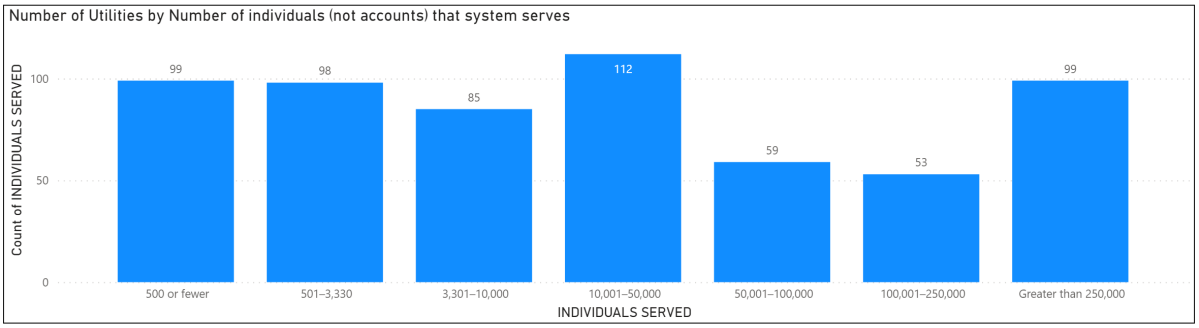
Count of NEED No assistance is needed by INDIVIDUALS SERVED



Service and Ownership Structure

PRIMARY SERVICE AND OWNERSHIP STRUCTURE

PRIMARY SERVICE	Department of a municipality or county	Private non-profit/cooperative	Privately owned or investor-owned	Special district or independent government entity	Total
Combined Drinking Water and Wastewater	196	12	15	77	**300**
Drinking Water Only	90	43	22	87	**242**
Wastewater Only	25	1	2	34	**62**
Total	**311**	**56**	**39**	**198**	**604**



51.4% of survey respondents are with a department of a **municipality** or county.

32.7% of survey respondents are with a **special district** or independent government entity.

9.3% of survey respondents are with a **private non-profit/cooperative**. **6.4%** of survey respondents are with a **privately-owned or investor-owned utility**.

49.8% of survey respondents represent **combined drinking water and wastewater systems**. **40%** of survey respondents represent **drinking water-only systems**. And **10.2%** of respondents represent **wastewater-only** systems.

PERCENT UTILITY 2021 BUDGET ALLOCATION FOR IT CYBERSECURITY	500 or fewer	501–3,330	3,301–10,000	10,001–50,000	50,001–100,000	100,001–250,000	Greater than 250,000	**Total**
1%–5%	6	19	18	26	20	12	29	**130**
6%–10%	1		4	10	4	6	12	**37**
Don't know	17	15	20	23	14	17	28	**134**
Greater than 10%	1	3	4	4		3	9	**24**
Less than 1%	64	54	33	33	13	11	14	**222**
Not applicable; IT cybersecurity is managed at the municipal or county government level	6	3	5	11	7	3	4	**39**
Total	**95**	**94**	**84**	**107**	**58**	**52**	**96**	**586**

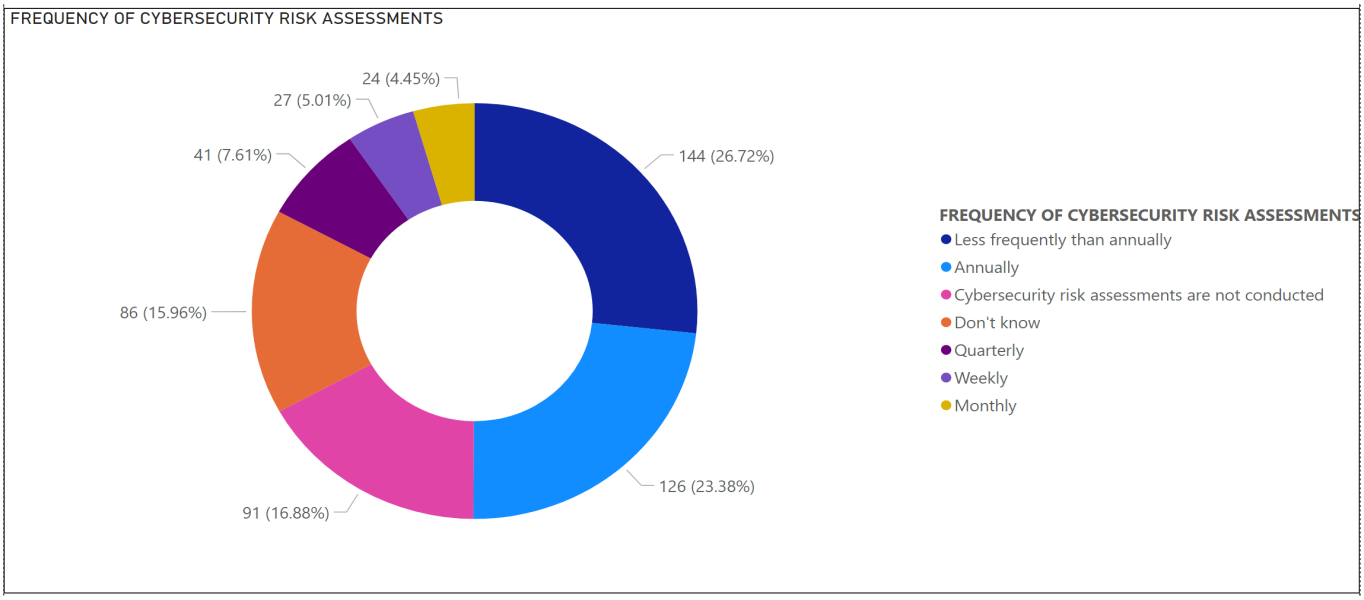
PERCENT UTILITY 2021 BUDGET ALLOCATION FOR OT CYBERSECURITY	500 or fewer	501–3,330	3,301–10,000	10,001–50,000	50,001–100,000	100,001–250,000	Greater than 250,000	**Total**
1%–5%	8	19	14	26	15	15	26	**123**
6%–10%			3	10	2	5	9	**29**
Don't know	19	17	21	25	12	13	30	**137**
Greater than 10%	1	1	3			2	3	**10**
Less than 1%	62	54	40	39	26	14	28	**263**
Not applicable; OT cybersecurity is managed at the municipal or county government level	5	3	3	8	3	3		**25**
Total	**95**	**94**	**84**	**108**	**58**	**52**	**96**	**587**

A representative sampling across all size systems provides the following 2021 budget allocations for cybersecurity:

- 38% of systems allocate less than 1% of budget to **IT** cybersecurity.
- 22.1% of systems allocate 1–5% of budget to **IT** cybersecurity.
- 6.3% of systems allocate 6-10% of budget to **IT** cybersecurity.
- 4.1% of systems allocate greater than 10% of budget to **IT** cybersecurity.
- 44.8% of systems allocate less than 1% of budget to **OT** cybersecurity.
- 20.95% of systems allocate 1–5% of budget to **OT** cybersecurity.
- 4.9% of systems allocate 6-10% of budget to **OT** cybersecurity.
- 1.7% of systems allocate greater than 10% of budget to **OT** cybersecurity.

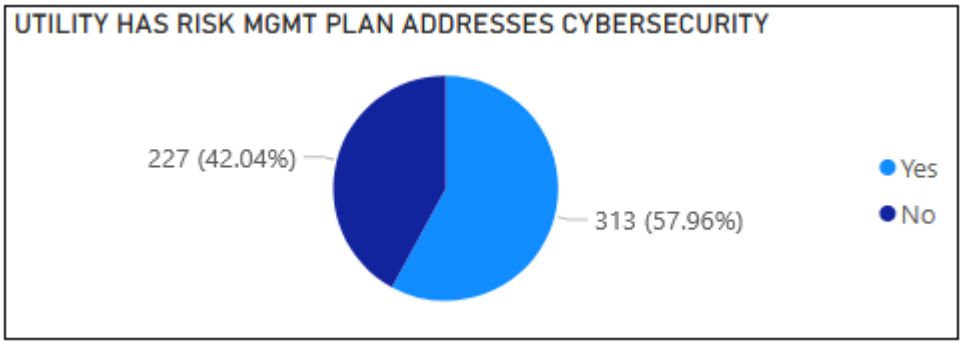
Frequency of Risk Assessments

Risk assessment is defined as the process of identifying risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of a system. Risk management includes threat and vulnerability analyses as well as analyses of adverse effects on individuals arising from information processing and considers mitigations provided by security and privacy controls planned or in place. Synonymous with risk analysis. [NIST SP 800-53r5]



23.38% of systems surveyed perform cybersecurity risk assessments annually. 7.61% of systems are conducting quarterly cybersecurity risk assessments and 5% of systems are conducting weekly cybersecurity risk assessments.

Risk Management Plans Addressing Cybersecurity



More than half of the systems surveyed (57.96%) have a risk management plan that addresses cybersecurity.

Risk Management Challenges

Responses varied by system type regarding risk management challenges. The **top three challenges by primary service** include:

- **Combined drinking water and wastewater systems**: 1. minimizing control system exposure; 2. assessing risks; and 3. identifying and remediation hardware or software vulnerabilities.
- **Drinking water systems**: 1. assessing risks; 2. awareness of cybersecurity threats and best practices; and 3. planning for emergencies, incidents and disasters.
- **Wastewater systems**: 1. minimizing control system exposure; 2. securing remote access to the OT system; and 3. assessing risks.

The **number one challenge** for systems serving more than 100,000 is **creating a cybersecurity culture within the utility**.

Awareness of threats and best practices was the top challenge for systems serving between 3,300 and 50,000 people.

Information-Sharing Concerns

The following high priority concerns were identified regarding the exchange of organizational information on cybersecurity threats, vulnerabilities, mitigation, and security incidents with external organizations:

ANSWER CHOICES	RESPONSES	
Lack of trust around my utility information being kept confidential	22.39%	118
Lack of credible information shared by other organizations	12.33%	65
Lack of know-how (who to share information with or how to do so)	37.76%	199
Lack of value, nothing gained in return	11.57%	61
None of the above (no barriers to information sharing with others)	30.36%	160
Don't know	16.89%	89
Total Respondents: 527		

Cybersecurity Program Challenges

Respondents gauged the extent that the following issues are a challenge for their organization's cybersecurity program. The purpose of this question was to capture elements of cybersecurity that are difficult to address.

	MINOR	←			SIGNIFICANT	TOTAL	WEIGHTED AVERAGE
Website security	34.78% 176	24.90% 126	21.74% 110	10.47% 53	8.10% 41	506	2.32
Information sharing	33.14% 168	21.89% 111	26.23% 133	11.83% 60	6.90% 35	507	2.37
Cloud security	28.46% 144	18.77% 95	26.09% 132	14.82% 75	11.86% 60	506	2.63
Physical security	24.11% 122	24.51% 124	26.68% 135	15.02% 76	9.68% 49	506	2.62
Incident response	19.08% 95	19.08% 95	25.90% 129	21.69% 108	14.26% 71	498	2.93
Awareness training program	18.38% 93	21.94% 111	27.67% 140	19.57% 99	12.45% 63	506	2.86
Device security	15.98% 81	23.27% 118	29.98% 152	19.33% 98	11.44% 58	507	2.87
Business continuity and disaster recovery	15.67% 79	19.05% 96	25.60% 129	20.83% 105	18.85% 95	504	3.08
Risk assessment and management	15.32% 78	18.07% 92	32.22% 164	20.04% 102	14.34% 73	509	3.00

IT- and OT-networked Assets

Information technology, or IT, refers to the business or enterprise network of a utility. This includes computers, software, firmware and similar procedures and services, such as email, websites, bill payment and customer management systems, and work order applications.

Operational technology, or OT, refers to required programmable systems that manage devices, monitor and control physical processes and events of a utility. OT includes industrial control systems, such as supervisory control and data acquisition (SCADA) systems; fire control systems; and physical access control mechanisms.

Identifying IT and OT assets is a critical first step in improving cybersecurity. An organization cannot protect what it cannot see.

37.9% of utilities have identified all IT-networked assets, with an additional 21.7% working to identify all IT-networked assets.

HAS UTILITY IDENTIFIED IT-NETWORKED ASSETS		500 or fewer	501–3,330	3,301–10,000	10,001–50,000	50,001–100,000	100,001–250,000	Greater than 250,000	Total
All IT-networked assets have been identified	1	12	12	26	44	23	30	56	**204**
Don't know		28	24	24	21	10	8	5	**120**
No work has been done to identify IT-networked assets		38	35	8	9	2	2	3	**97**
Work is underway to identify IT-networked assets		6	15	20	24	20	12	20	**117**
Total	**1**	**84**	**86**	**78**	**98**	**55**	**52**	**84**	**538**

30.5% of utilities have identified all OT-networked assets, with an additional 22.5% working to identify all OT-networked assets.

HAS UTILITY IDENTIFIED OT-NETWORKED ASSETS		500 or fewer	501–3,330	3,301–10,000	10,001–50,000	50,001–100,000	100,001–250,000	Greater than 250,000	Total
All OT-networked assets have been identified	1	8	9	21	35	19	31	40	**164**
Don't know		31	28	28	29	13	7	13	**149**
No work has been done to identify OT-networked assets.		40	37	9	9	3	4	1	**103**
Work is underway to identify OT-networked assets		5	12	19	25	20	10	30	**121**
Total	**1**	**84**	**86**	**77**	**98**	**55**	**52**	**84**	**537**

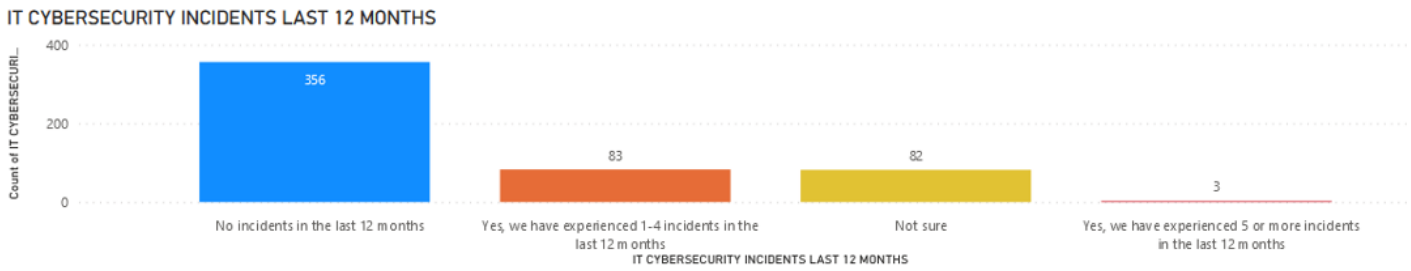
The following responses were provided in response to the question "For identified networked IT and OT assets, what is the status of your utility's cyber protection efforts?"

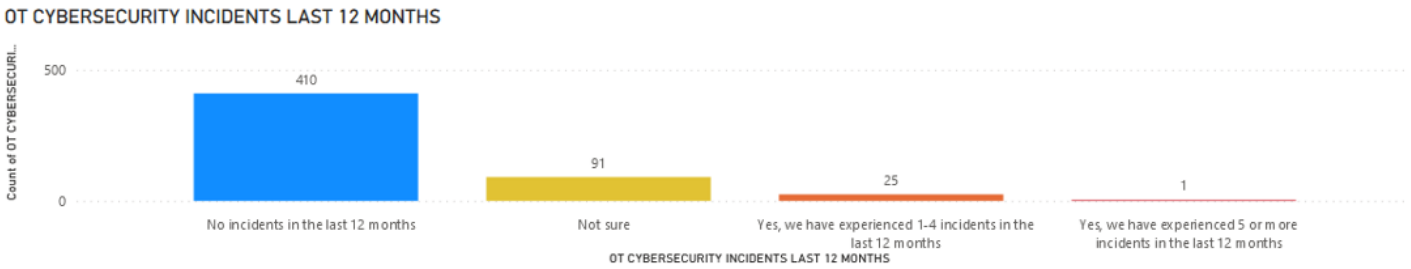
Nearly 75% of respondents report they have implemented efforts or are in some stage of progress.

ANSWER CHOICES	RESPONSES	
No progress/no current plans to conduct cyber protection efforts	25.47%	135
Planning to conduct cyber protection efforts	15.47%	82
Cyber protection efforts are in progress	36.60%	194
Cyber protection efforts have been implemented and are monitored regularly	22.45%	119
TOTAL		530

IT cybersecurity incident: A violation or imminent threat of violation to the confidentiality, integrity, or availability of IT systems and/or data.

OT cybersecurity incident: A violation or imminent threat of violation to the availability, integrity, or confidentiality of OT systems and/or data.





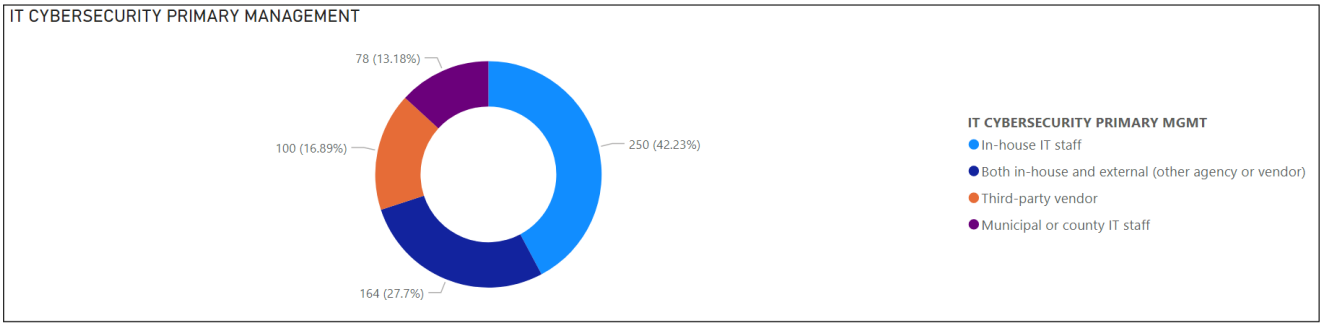
67.9% of systems reported no IT cybersecurity incidents in the last twelve months.

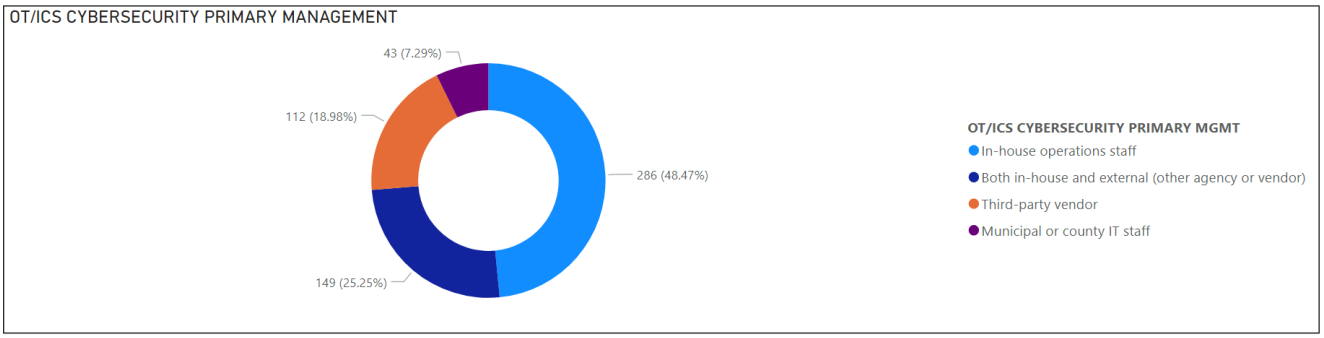
15.8% of systems reported having experienced 1 to 4 IT cybersecurity incidents in the last twelve months.

77.8% of systems reported no OT cybersecurity incidents in the last twelve months.

4.7% of systems reported having experienced 1 to 4 OT cybersecurity incidents in the last twelve months.

IT and OT Management and Workforce



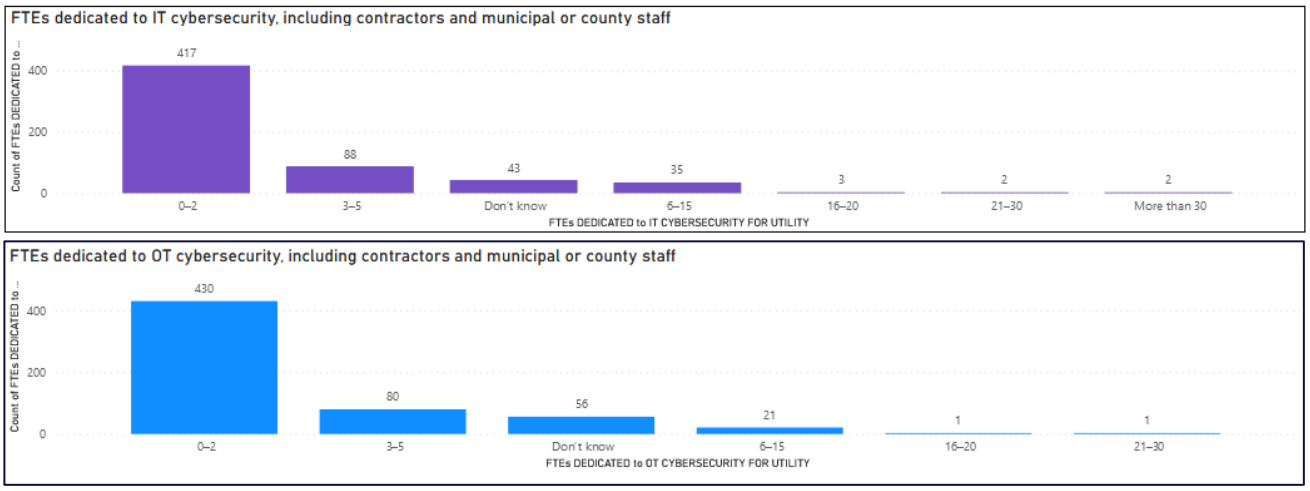


42% of utility IT cybersecurity is primarily managed by in-house IT staff. 27.7% of utility IT cybersecurity is primarily managed by both in-house and external vendors or other agencies. 16.89% of utility IT cybersecurity is primarily managed by third-party vendors. And 13.18% of utility IT cybersecurity is primarily managed by municipal or county IT staff.

48.47% of utility OT/ICS cybersecurity is primarily managed by in-house IT staff. 25.25% of utility OT/ICS cybersecurity is primarily managed by both in-house and external vendors or other agencies. 18.98% of utility OT/ICS cybersecurity is primarily managed by third-party vendors. And 7.29% of utility OT/ICS cybersecurity is primarily managed by municipal or county IT staff.

63.8% or respondents provided that their utility does not employ a Chief Information Security Officer (CISO) or equivalent. 21.9% of utilities have a CISO or equivalent. 8% of respondents noted that the role resides with their municipal or county government.

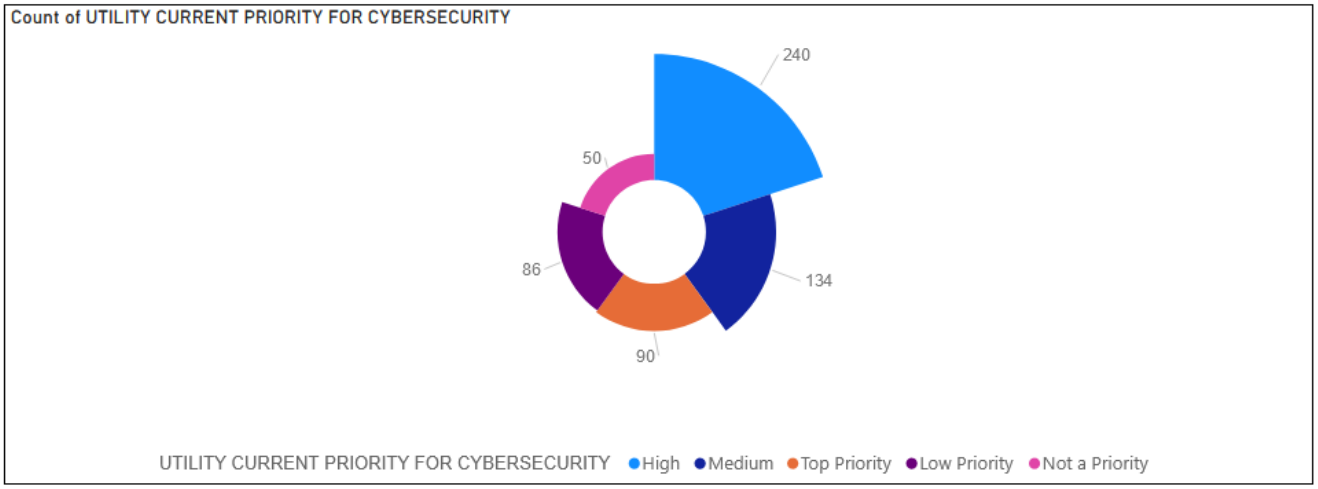
FTEs dedicated to cybersecurity include the following:



70.67% of respondents noted 0-2 FTEs dedicated to IT cybersecurity, and 73% of respondents noted 0-2 FTEs dedicated to OT cybersecurity. Additionally, the larger the utility the larger the increase in FTEs dedicated to cybersecurity.

Current Focus on Cybersecurity as a Priority

UTILITY CURRENT PRIORITY FOR CYBERSECURITY	500 or fewer	501–3,330	3,301–10,000	10,001–50,000	50,001–100,000	100,001–250,000	Greater than 250,000	Total
High	9	16	40	60	33	33	49	240
Low Priority	33	27	8	7	5	4	2	86
Medium	1 16	32	22	26	11	7	19	134
Not a Priority	34	8	7				1	50
Top Priority	5	14	8	18	10	9	26	90
Total	**1 97**	**97**	**85**	**111**	**59**	**53**	**97**	**600**



55% of respondents ranked cybersecurity is a high or top priority. 22.3% consider cybersecurity a medium priority, while 22.6% - mainly systems serving 3,300 people or fewer- ranked cybersecurity a low priority or not a priority.

Cybersecurity Resources Used in the Sector

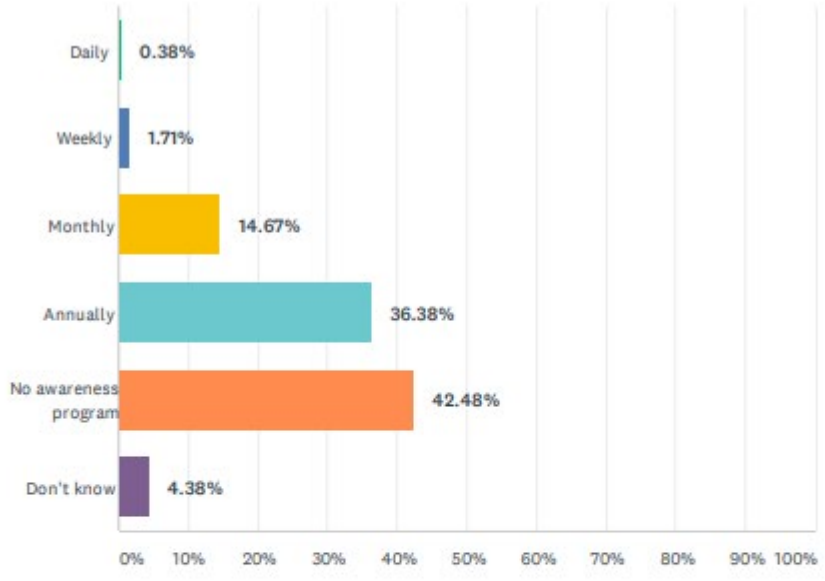
The top 5 cybersecurity resources used by utilities include the

- AWWA Cybersecurity Guidance (based on CSF)
- WaterISAC 15 Cybersecurity Fundamentals for Water and Wastewater Utilities
- NIST Cybersecurity Framework (CSF)
- DHS CISA Cybersecurity Assessment Tool (CSET) and other services
- NIST SP 800-82 Guide to Industrial Control Systems Security

Resources not covered by the survey include the U.S. Environmental Protection Agency's Cybersecurity Incident Action Checklist and its cybersecurity assessment program.

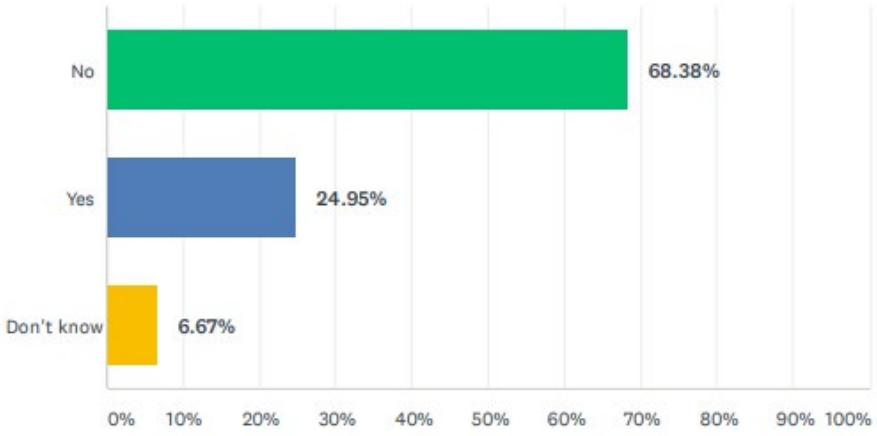
Training

More than 50% of utilities conduct cybersecurity awareness training for utility staff:



ANSWER CHOICES	RESPONSES	
Daily	0.38%	2
Weekly	1.71%	9
Monthly	14.67%	77
Annually	36.38%	191
No awareness program	42.48%	223
Don't know	4.38%	23
TOTAL		525

The following provides that nearly 25% of utilities participate in cybersecurity-related tabletop exercises, mock drills, technology failure exercises or emergency management exercises:



ANSWER CHOICES	RESPONSES	
No	68.38%	359
Yes	24.95%	131
Don't know	6.67%	35
TOTAL		525

Next Steps

Drinking water and wastewater utilities and the thousands of employees that run them are public health guardians and environmental protectors, treating drinking water to standards that meet state and federal regulations, ensuring wastewater treatment practices protect water bodies, and ensuring these vital services can continue in times of crisis.

On the whole, the sector recognizes the importance of investing in cybersecurity and adopting cybersecurity best practices. Many utilities are highly advanced, with expert IT and OT managers, keeping their devices, networks and consumers safe. Others, as shown in these results, require assistance to enhance their IT and OT cybersecurity. The sector itself also continues to support national cybersecurity efforts by collaborating with federal partners, developing its own sector-specific cybersecurity resources, and operating the Water Information Sharing and Analysis Center.

The challenges and needs outlined by respondents here offer guideposts for next steps by the Water and Wastewater Systems sector, Congress, federal agencies, and their partners.