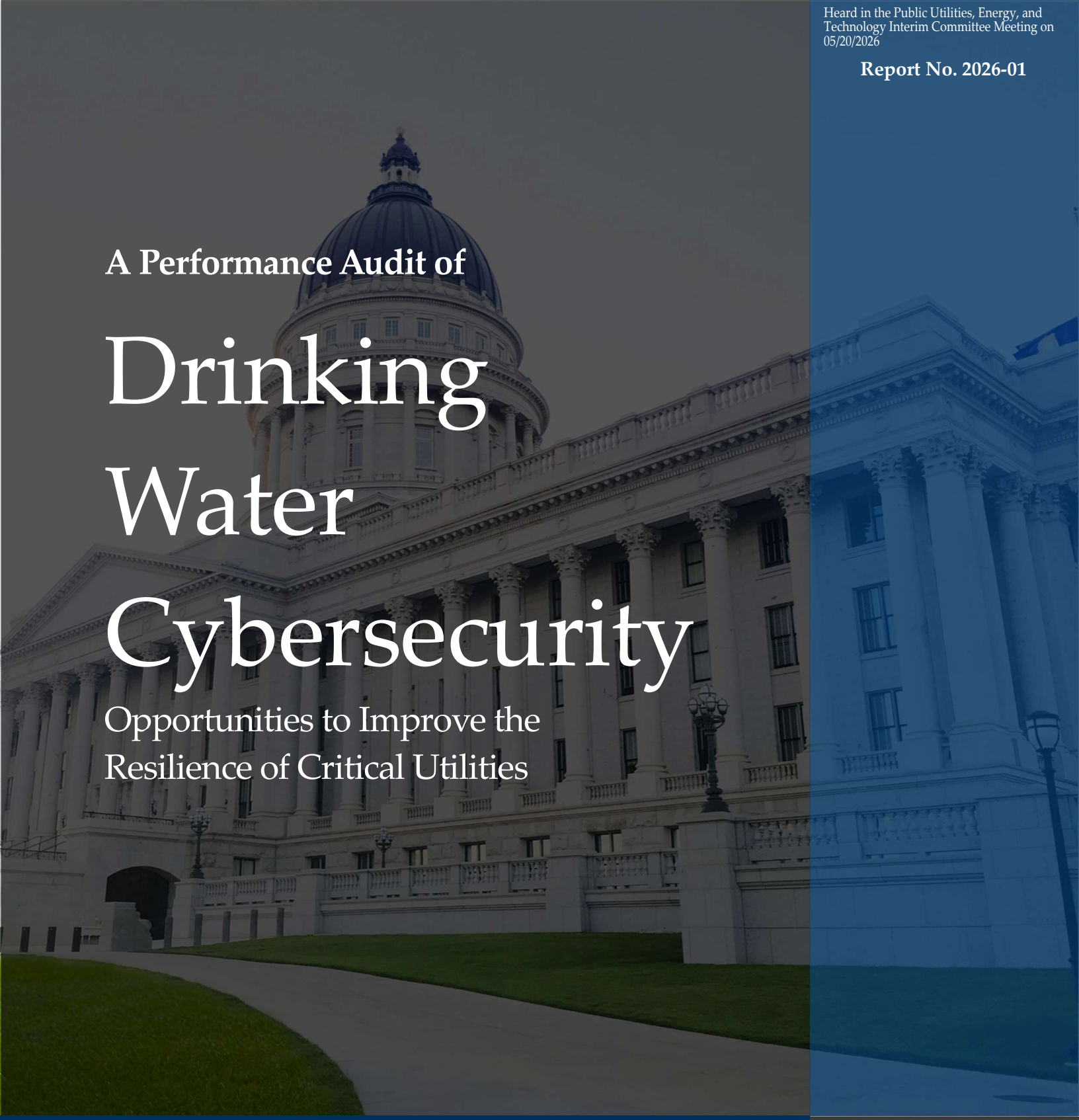
Heard in the Public Utilities, Energy, and Technology Interim Committee Meeting on 05/20/2026

Report No. 2026-01



A Performance Audit of

Drinking Water Cybersecurity

Opportunities to Improve the Resilience of Critical Utilities

Office of the Legislative Auditor General

Report to the **UTAH LEGISLATURE**

LEGISLATIVE AUDITOR GENERAL

LEGISLATIVE
AUDITOR GENERAL

Audit Subcommittee

President J. Stuart Adams, Co-Chair
President of the Senate

Senator Kirk Cullimore
Senate Majority Leader

Senator Luz Escamilla
Senate Minority Leader

Speaker Mike Schultz, Co-Chair
Speaker of the House

Representative Casey Snider
House Majority Leader

Representative Angela Romero
House Minority Leader

Audit Staff

Kade R. Minchey, Auditor General, CIA, CFE

Jesse Martinson, Manager, CIA

Christopher McClelland, Audit Supervisor, CIA, CFE

Brandon Checketts, Audit Staff

Office of the Legislative Auditor General

Kade R. Minchey, Legislative Auditor General

450 N State Street, Suite N385 | Salt Lake City, UT 84114 | Phone: 801.538.1033

Audit Subcommittee of the Legislative Management Committee

President J. Stuart Adams, Co-Chair | Speaker Mike Schultz, Co-Chair

Senator Kirk Cullimore | Representative Casey Snider

Senator Luz Escamilla | Representative Angela Romero

January 30, 2026

TO: THE UTAH STATE LEGISLATURE

Transmitted herewith is our report:

"A Performance Audit of Drinking Water Cybersecurity" [Report #2026-01].

An audit summary is found at the front of the report. The scope and objectives of the audit are included in the audit summary.

Utah Code 36-12-15.3(2) requires the Office of the Legislative Auditor General to designate an audited entity's chief officer. Therefore, the designated chief officer for the Utah Department of Environmental Quality is Tim Davis. Mr. Davis has been notified that they must comply with the audit response and reporting requirements as outlined in this section of ***Utah Code***.

We will be happy to meet with appropriate legislative committees, individual legislators, and other state officials to discuss any item contained in the report in order to facilitate the implementation of the recommendations.

Sincerely,

Kade Minchey

Kade R. Minchey, CIA, CFE

Auditor General

kminchey@le.utah.gov

LEGISLATIVE AUDITOR GENERAL

AUDIT SUMMARY

REPORT 2026-01 | JANUARY 2026

Office of the Legislative Auditor General | Kade R. Minchey, Auditor General

PERFORMANCE AUDIT

DRINKING WATER CYBERSECURITY

AUDIT REQUEST

The Legislative Audit Subcommittee prioritized an audit of cybersecurity readiness throughout the state of public utilities in its October 2024 meeting. This audit focuses on drinking water while future audits will look at other public utilities.

BACKGROUND

Drinking water systems provide water that satisfies physical needs and supports other critical infrastructure like electricity generation and hospitals. Water systems tend to incorporate operational technology that enables operators to remotely control and monitor physical processes like valves and pumps. While technology has reportedly increased reliability and efficiency, it has also increased cybersecurity risks. Actual cyberattacks have led to water disruptions and recovery costs.

KEY FINDINGS

1.1 Drinking water systems can do more to prioritize cybersecurity and implement best practices.

RECOMMENDATIONS

1.1 The Utah Drinking Water Board should require all community water systems that use operational technology to adopt a plan to implement cybersecurity best practices like those outlined by the U.S. Environmental Protection Agency. Plans should target baseline best practices to provide a solid foundation for cybersecurity.

1.2 The Legislature should consider whether any additional steps should be taken to further address cybersecurity risk to drinking water systems.

1.3 The Legislature should consider modifying statute to require drinking water systems that have governing bodies to provide regular cybersecurity briefings to their governing council or board. Briefings should include information on existing protections, cybersecurity risk, and the results of any cybersecurity assessments completed.

REPORT SUMMARY

Utah Drinking Water Systems Need to Better Prepare for a Cyberattack

Utah's drinking water systems are not fully implementing basic cybersecurity practices established by the U.S. Environmental Protection Agency, leaving water systems vulnerable to cyberattack. In 2023, a Utah municipality suffered a cyberattack that forced their water system to operate in manual mode for three weeks and cost $360,000 to recover and repair. We sent out a survey to more than 500 water system contacts in the state and found opportunities to improve vulnerability management, risk assessments, training, and incident response plans. Assessments conducted by the Utah Education and Telehealth Network confirmed similar findings that many systems lack foundational protections against growing cyber threats.

Water systems do not appear to be following two best practices of governance: actively engaged governing boards and strategic planning. We believe better governance practices will enable drinking water systems to better address cybersecurity risks. We recommend that the Utah Drinking Water Board require all community water systems using operational technology to adopt plans targeting cybersecurity best practices. We also recommend the Legislature consider modifying statute to require systems with governing bodies to provide regular cybersecurity briefings to their councils or boards.

Assessments Point to Opportunities to Improve Key Cybersecurity Practices in Water Systems

We partnered with the Utah Education and Telehealth Network to test some prioritized cybersecurity best practices in a sample of Utah drinking water systems. These tests demonstrated that Utah water systems can improve key cybersecurity controls.

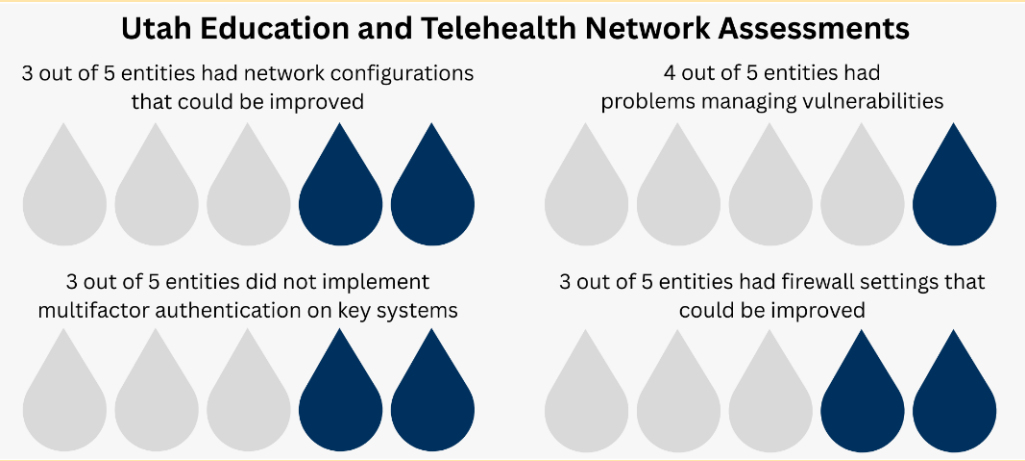


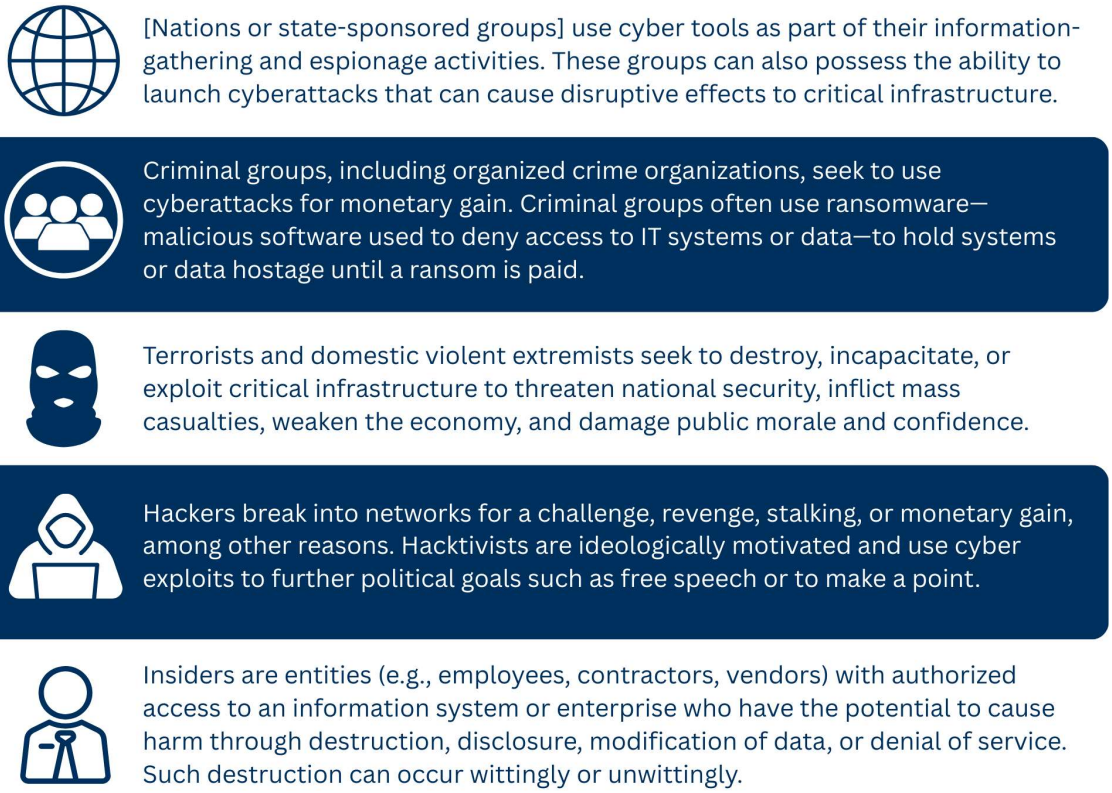
Table of Contents

Introduction

Society needs clean and reliable drinking water to function. Not only does it meet basic physical needs, but it also supports other critical infrastructure like electricity generation. Drinking water systems generally rely on technology to operate, which also makes them vulnerable to cyberattacks. This report focuses on the cybersecurity controls of Utah's drinking water systems and provides possible recommendations to drive improvement.

Critical Infrastructure Is Increasingly Under Attack from a Variety of Cyber Threat Actors

As drinking water systems integrate more digital technologies, their exposure to cyber threats grows. Between January 2023 and January 2024, the world's critical infrastructure was attacked more than 420 million times (13 attacks per second), a 30% increase from 2022. Threat actors have access to improved technology, and cyberattacks have become more sophisticated. The following infographic contains information from the U.S. Government Accountability Office about cyber threat actors:

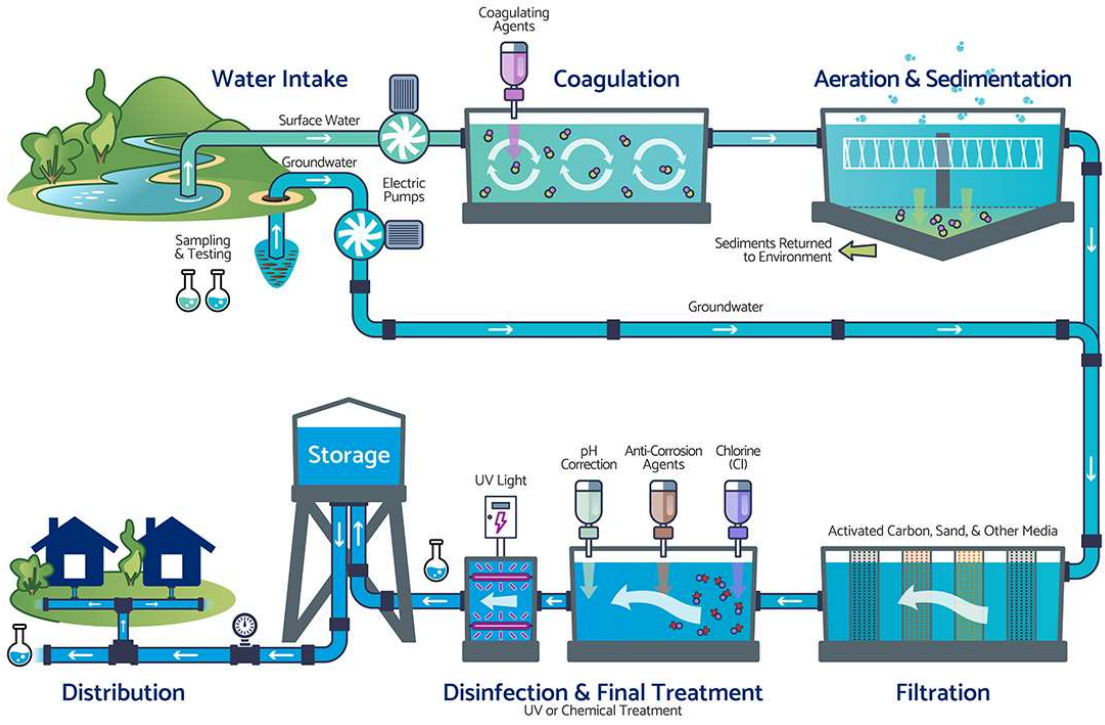


Source: U.S. Government Accountability Office, Critical Infrastructure Protection: EPA Urgently Needs a Strategy to Address Cybersecurity Risks to Water and Wastewater Systems.

It is important to note that the number of critical infrastructure cyberattacks includes only those that have been reported. Those in charge of critical infrastructure may be unaware of reporting requirements or be reluctant to report attacks. Therefore, the risk of cyberattacks on Utah drinking water systems may be higher than the data suggests.

Complicated Equipment and Processes Control Drinking Water Systems

Drinking water systems generally have three main components: water sources, water treatment, and water distribution. Drinking water comes from surface sources like lakes or groundwater from wells. Water is treated and disinfected based on its source. It is then put into storage that ensures adequate reserves and water pressure. The following infographic briefly summarizes key components of local drinking water systems:



Source: Corix Utilities, Texas. Not all aspects of this infographic may be applicable to Utah water systems.

Pumps move water through the system, including into storage that uses gravity to get the water to users. Valves maintain desired pressure and help shut off water to different parts of the system for maintenance. Figure 1 shows pumps and a pressure-regulating valve at a booster station at a Utah drinking water system. A booster station is used to move water to a storage tank at a higher elevation.

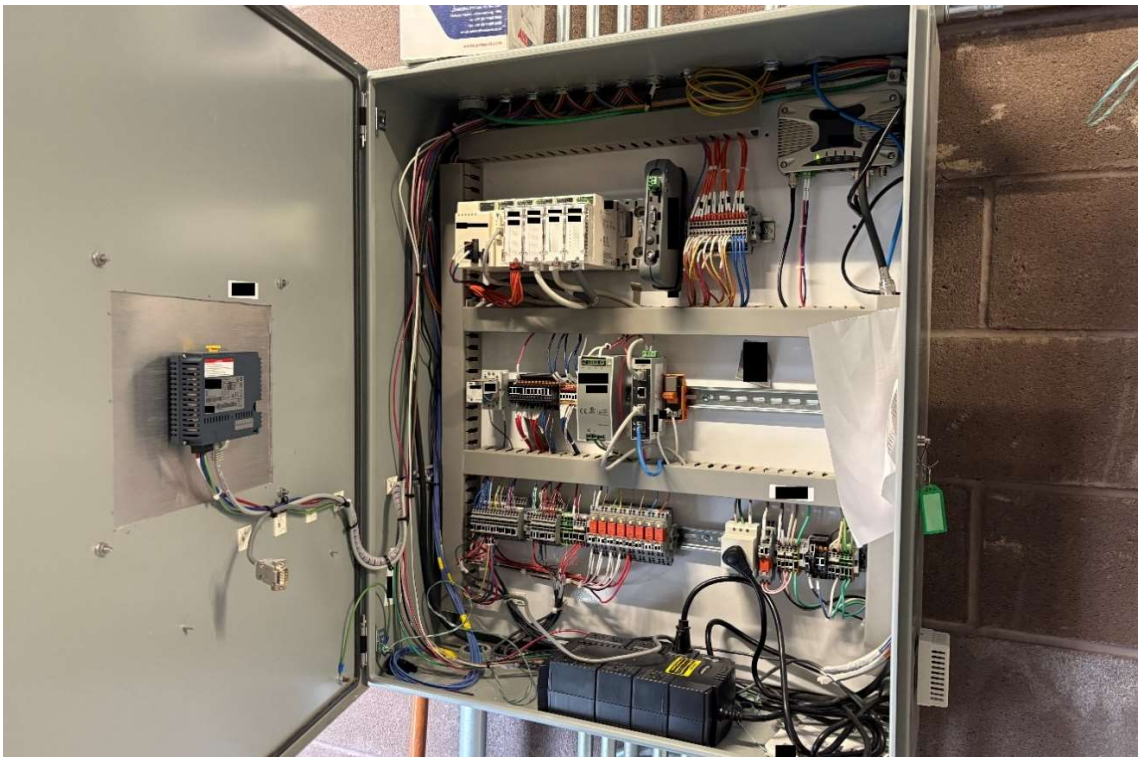
Figure 1 Pumps (Left Picture) and Valves (Right Picture) Move and Regulate Water Flow in Drinking Water Systems. These pictures come from a local drinking water system.

Source: Auditor generated.

Drinking water systems generally use operational technology (OT) to control or monitor physical processes like pumps and valves. This technology can provide benefits such as real-time monitoring, automated controls, and improved efficiency. While OT may have improved operations, it has also increased the cyber risk to water systems. Priority best practices, discussed in Chapter 1 of this report, describe the first steps for protecting OT and drinking water systems. Figure 2 shows an example of OT equipment that helps automate processes at a local drinking water system.

Priority best practices, discussed in Chapter 1 of this report, describe the first steps for protecting operational technology and drinking water systems.

Figure 2 This Operational Technology, Known as Programmable Logic Controllers, Helps Automate Processes for Drinking Water Systems. This picture comes from a local drinking water system. This equipment helps operate the booster station that moves water to a higher altitude storage tank.



Source: Auditor generated.

During the course of the audit, we partnered with cybersecurity experts to assess five drinking water systems in the state. We also surveyed all of Utah's community water systems[1] about cybersecurity controls and governance. In Chapter 1 of this report, we compared these two sources of information against cybersecurity best practices published by the U.S. Environmental Protection Agency. We found that governing boards of individual water systems should be more involved in cybersecurity planning and ensuring adequate controls are in place. In future audits, we will discuss OT cybersecurity for other public utilities.

We found that governing boards of water systems should be more involved in cybersecurity planning and ensuring adequate controls are in place.

[1] For the purposes of this report, *drinking water systems* refers to community water systems that have 15 or more year-round service connections or 25 or more year-round residents. Community water systems make up almost half of all water systems in Utah but serve over 3 million residents.

Chapter 1
Utah Drinking Water Systems Need to Better Prepare for a Cyberattack

Utah's drinking water entities can do more to follow cybersecurity best practices. The adoption of technology has created vulnerabilities that can impact the safety and availability of drinking water. Opportunities to improve cyber controls appear to stem from poor governance among the governing bodies[2] that oversee the state's local drinking water systems.[3] When briefings do occur, they are typically triggered as needs arise rather than being part of a structured process. Infrequent briefings are concerning because cyber threats on critical infrastructure grow and evolve, and drinking water entities need to ensure they are adequately protected. The Utah Drinking Water Board can do more to require water systems to develop plans to adopt cyber best practices. The Legislature should consider strengthening requirements on governing bodies overseeing water systems to ensure they are addressing cybersecurity risk.

Opportunities to improve cyber controls appear to stem from poor governance among the governing bodies that oversee the state's local drinking water systems.

This report discusses important cybersecurity improvements needed to help ensure the safety and security of Utah's drinking water. We intentionally present our findings at a high level to avoid drawing attention to specific security vulnerabilities. In addition, we provided a draft of the report to the principal water systems we audited to allow them time to address any identified concerns before the report is made public. Governing boards and water system leaders must remain continually diligent in strengthening and maintaining cybersecurity protections.

---

[2] A board of trustees oversees special districts like water conservancy districts. Municipalities have either a city commission, city council, or town council as a governing body. However, a subset of water systems may not have a governing body.

[3] For the purposes of this report, *drinking water systems* refers to community water systems that have 15 or more year-round service connections or 25 or more year-round residents. Community water systems make up almost half of all water systems in Utah but serve over 3 million residents.

1.1 Drinking Water Systems Can Do More to Prioritize Cybersecurity and Implement Best Practices

Utah's drinking water systems frequently use operational technology (OT) as part of their operations and also frequently have room to improve key cybersecurity controls.[4] This technology helps systems remotely control or monitor physical processes like valves and pumps. Needed improvements in cybersecurity appear to be an issue of governance. Typically, water systems appear to be operated by cities or special districts, political subdivisions that report to governing bodies. Infrequent briefings to boards and councils indicate governing bodies are not as involved as they could be in cybersecurity or planning for improvements. The Utah Legislature should consider taking steps to help improve governance of drinking water systems by requiring regular cybersecurity briefings. In addition, the Utah Drinking Water Board can help drive improvement by requiring drinking water systems to make plans to improve cybersecurity.

Cyberattacks Can Disrupt the Reliable Delivery of Safe Drinking Water

Modern drinking water systems increasingly rely on internet-connected technology to monitor and control water distribution. While this technology has reportedly increased water system efficiency, it also introduces risks. Internet-connected systems create potential points of entry for cyber threat actors who can exploit vulnerabilities to disrupt operations or compromise sensitive data. The following infographic summarizes possible consequences of cyberattacks on drinking water systems:

Modern drinking water systems increasingly rely on internet-connected technology to monitor and control water distribution.

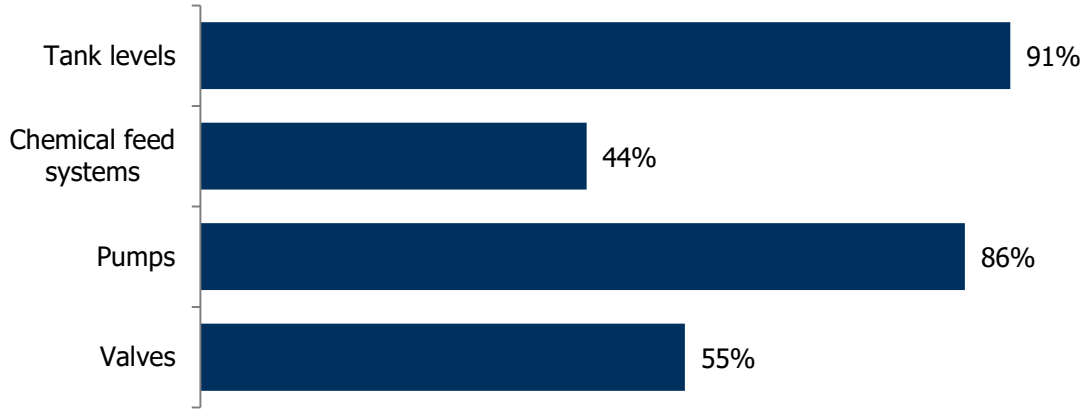
[4] Operational technology is used to control or monitor physical processes. See the Introduction in this report for more information.

Source: U.S. Government Accountability Office, Environmental Protection Agency, Lark, Kaspersky, Cornell University, Clemson University, Federal Bureau of Investigation, Cybersecurity & Infrastructure Security Agency.

Our water systems may be vulnerable to cyberattack because networked technology is now commonly used to operate them. In the last ten years, a drinking water system in Utah experienced a chemical overfeed in its water system, which had potential health impacts.[5] This was not caused by a cyberattack. However, the design of the water system, including remote control of chemical dosing, created a vulnerability that could have been exploited by an attacker under certain circumstances. Figure 1.1 highlights the parts of drinking water systems in Utah that can be monitored or controlled by OT and may be vulnerable to attack.

[5] A baby reportedly vomited as a result of drinking formula made from impacted water. Higher chemical concentrations also had the potential to leach metals like lead from water pipes into the drinking water.

Figure 1.1 Drinking Water Equipment in Utah May Be Vulnerable to Cyberattacks Because It Can Be Monitored or Controlled Through Technology. The results from a survey of Utah's drinking water systems show the parts of water systems that can be controlled or monitored through operational technology.

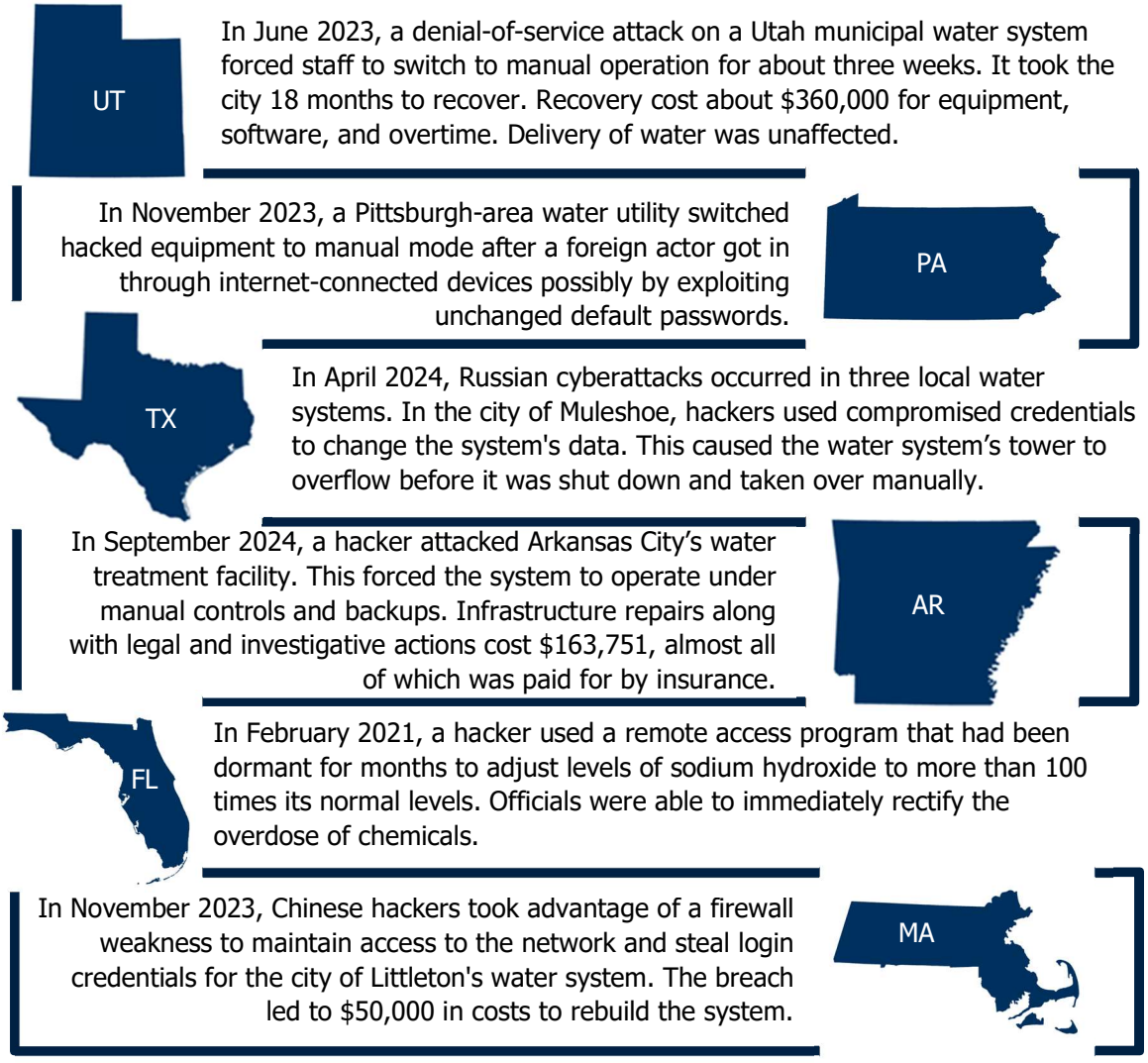


Source: Auditor generated from survey sent to 507 community water system contacts. This question had 117 respondents.

These components ensure a reliable supply of safe drinking water. Both large and small water systems in Utah currently use OT to provide drinking water. Cyber threat actors could make water unsafe to drink or stop the flow of water if some of these systems are compromised. According to the Utah Division of Drinking Water, these attacks can also cause significant financial impacts and operational continuity challenges. This often requires additional manpower and resources to operate, maintain, and restore drinking water operations.

Cyber Threat Actors Have Targeted Water Utilities, Both Big and Small, Around the United States

In Utah, a recent attack on a municipal water system highlighted that even local utilities are vulnerable. Similar attacks in other states have resulted in service interruptions, financial losses, and public safety concerns. The examples we discuss in the following infographic demonstrate that water systems are a target for cyber threats and the consequences of actual attacks:



Source: Conversation with local Utah water system, Pittsburgh NPR News Station WESA, Water ISAC, AP News, KSN News, CNN News, Boston.com, conversation with Texas public works.

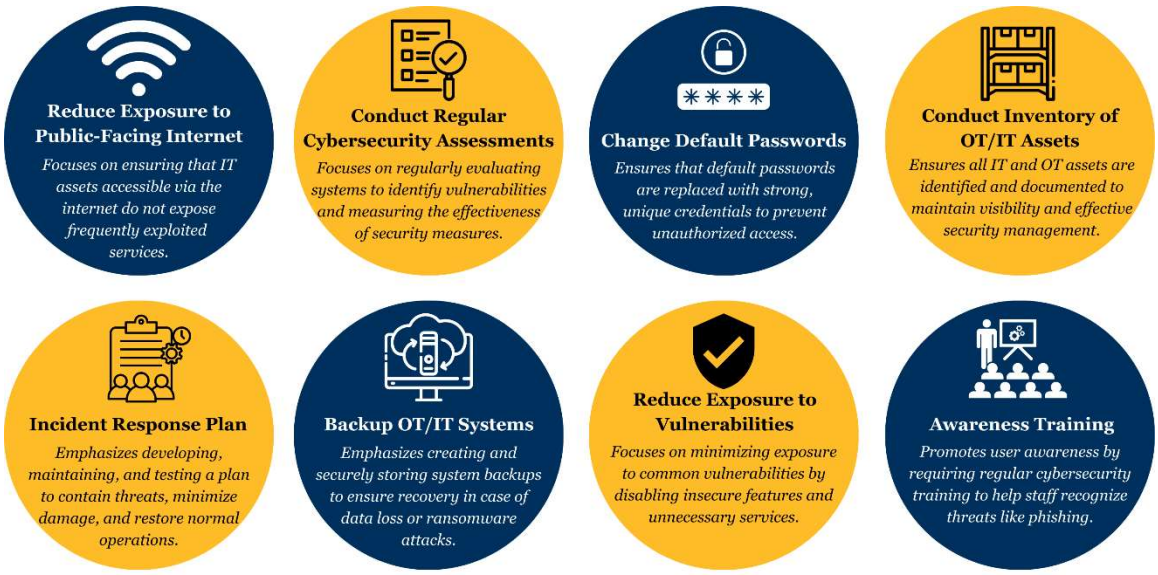
Drinking water systems not only supply vital water to citizens but support other critical infrastructure sectors as well. Hospitals, electricity-generating facilities, and emergency services all depend on a reliable water supply. A successful cyberattack on a water system could have cascading effects, disrupting multiple sectors and threatening public health and safety.

Drinking Water Systems Are Not Implementing Cybersecurity Best Practices

Results from detailed assessments and a survey indicate Utah's drinking water systems could do more to implement cybersecurity best practices.[6] The U.S.

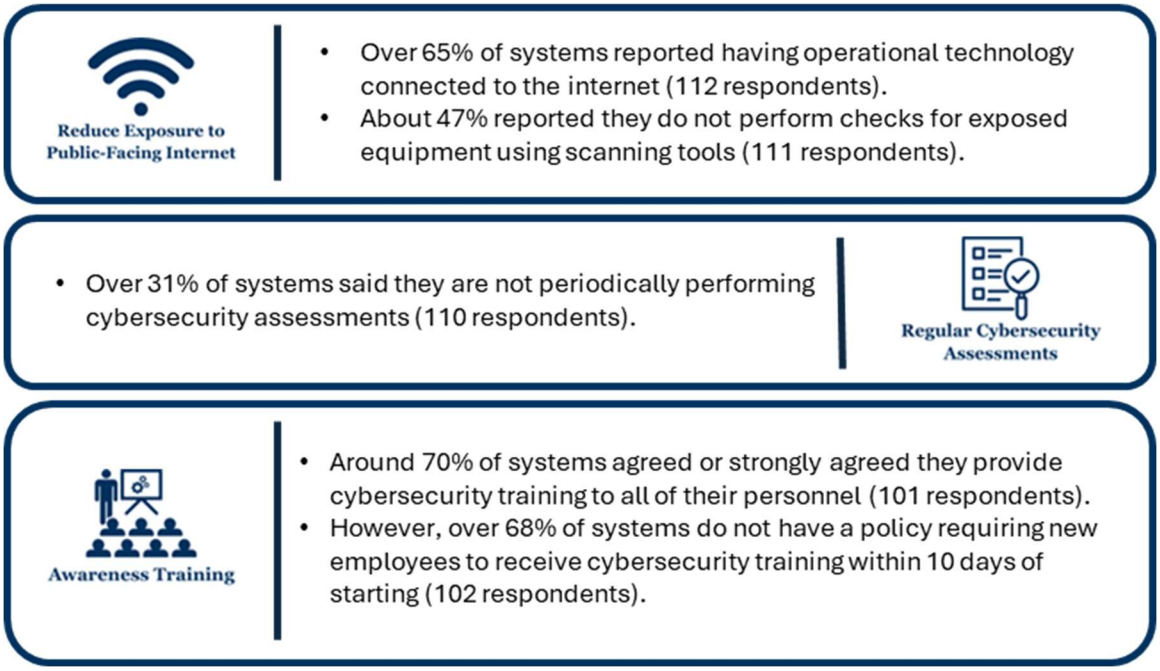
[6] We designed the assessments and survey to measure implementation of priority practices published by the U.S. Environmental Protection Agency for drinking water systems. These

Environmental Protection Agency's (EPA) best practices are known to reduce the risk of cyberattacks and have been applied across infrastructure sectors. The following infographic summarizes EPA's eight priority practices:

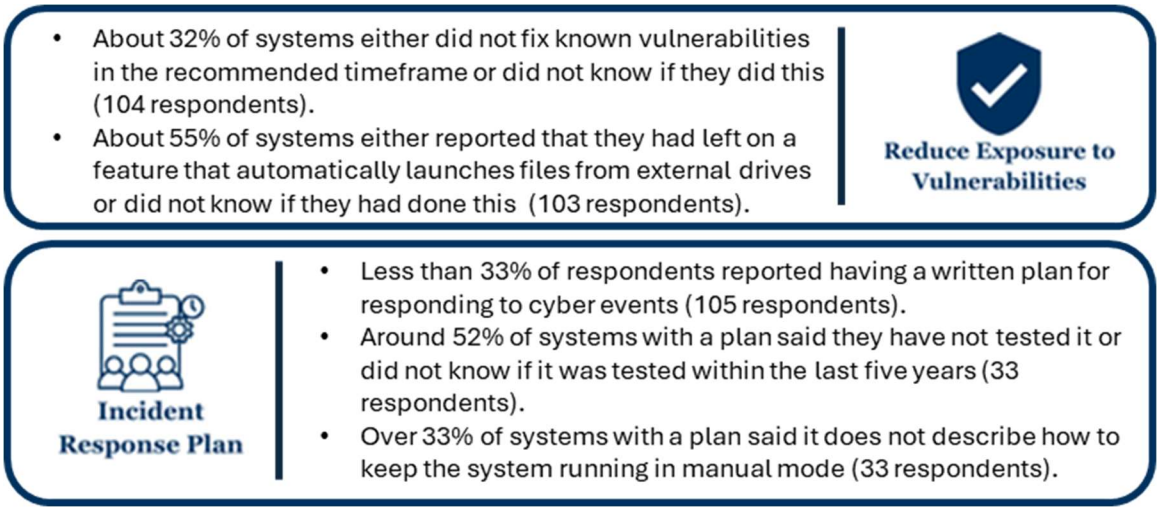


Source: U.S. Environmental Protection Agency.

The survey results below highlight opportunities for Utah drinking water systems to improve the implementation of EPA's priority practices:



practices are a subset of Cross-Sector Cybersecurity Performance Goals published by the Cybersecurity & Infrastructure Security Agency.



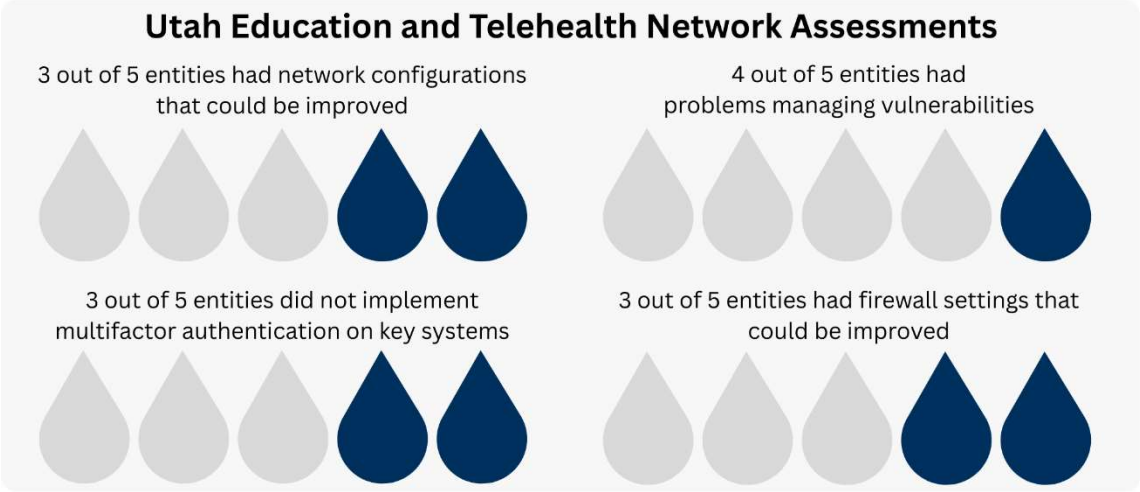
Source: Auditor generated from survey administered by the Office of the Legislative Auditor General.

When looking at the survey results by size of water system, smaller systems generally report slightly lower implementation of best practices compared to larger systems. Given that a Utah municipality had to operate in manual mode for three weeks after a cyberattack, the last point on incident response plans is concerning. Less than a third of survey respondents reported having a plan to respond to cyber events, and one-third of those did not include procedures for how to operate in manual mode. In addition, about half of those with a plan either had not practiced it or didn't know if they had practiced it, which is notable because practicing is essential to an effective incident response.

Drinking water systems should focus on cybersecurity and key cybersecurity controls.

Drinking water systems should focus on cybersecurity and key cybersecurity controls. For example, training ensures that staff can recognize and respond to phishing attempts and other common attack vectors. Incident response plans provide a structured approach for containing and recovering after an attack. Plans help reduce downtime and public health risks, help water systems recover quickly, and ensure continuous service. Vulnerability scanning helps utilities identify and fix weaknesses before they can be exploited. These measures are critical because they address both prevention and response, which strengthen the overall security of water systems.

In addition to conducting the survey, we partnered with the Utah Education and Telehealth Network (UETN) to validate certain cybersecurity controls of five drinking water systems around the state. These assessments looked at best practices that help reduce risk in the drinking water sector. Three or more of the observed drinking water systems could improve in the following areas:



Source: Drinking water system assessments conducted by the Utah Telehealth and Education Network.

These results are concerning. UETN's assessments validated survey responses that managing vulnerabilities is an issue. Proper network configuration is important because it limits the spread of an attack by separating critical systems. Multifactor authentication adds an extra layer of protection beyond passwords, making it harder for unauthorized users to gain access. Firewall settings control what traffic enters or leaves a network, helping block unnecessary or risky connections.

Needed Improvements to Cybersecurity Controls Can Be Attributed to Poor Governance

Water systems do not appear to be following two best practices of governance: actively engaged governing boards and strategic planning. This could explain the needed improvements in cybersecurity discussed earlier. Water systems report not regularly briefing their governing bodies on cybersecurity and not having long-term plans to improve cybersecurity. We believe better governance practices will enable drinking water systems to better address cybersecurity risks. The Utah Drinking Water Board and the Legislature should consider taking steps to require drinking water systems to improve governance.

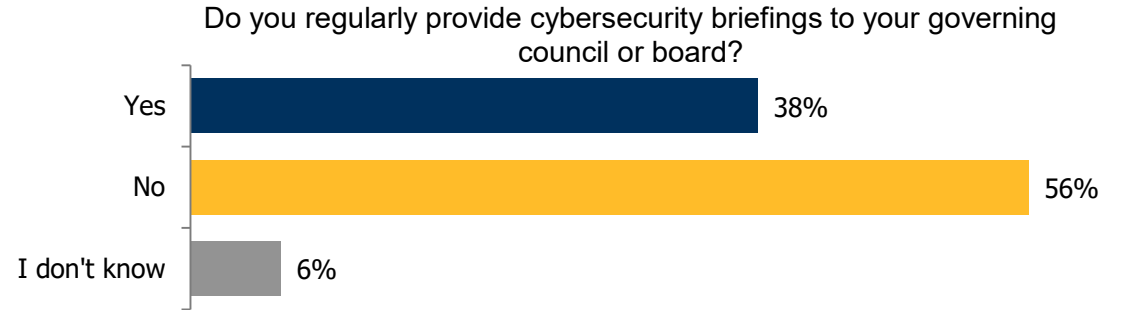
Water systems do not appear to be following two best practices of governance: actively engaged governing boards and strategic planning.

Water systems operated by municipalities and special districts serve a significant amount of Utah's population, and statute requires them to operate under governing bodies.[7] However, these governing

[7] Other water systems appear to be associated with homeowners' associations or private companies. The Utah Division of Drinking Water reports that some smaller community water systems do not have governing bodies.

bodies do not appear to be heavily involved in cybersecurity. Figure 1.2 shows the results from a question we asked water systems about briefing governing boards and councils.

Figure 1.2 Water Systems Report Not Regularly Briefing Their Governing Board or Council on Cybersecurity. Water systems tend to update their governing bodies as the need arises.



Source: Auditor generated from survey sent to 507 community water system contacts. The question had 116 respondents.

The results for this question were similar for both large and small drinking water systems. In addition, despite opportunities to improve cyber controls, water systems also report that they do not have long-term plans to improve cybersecurity. Almost 38% of respondents indicated that they do not have a multiyear plan to improve cybersecurity. The limited involvement of governing bodies is concerning because they should play critical roles in ensuring the organizations they oversee function properly.

Almost 38% of survey respondents indicated that they do not have a multi-year plan to improve cybersecurity.

When looking at internal controls for government agencies, the U.S. Government Accountability Office details the role of oversight bodies that oversee management decisions. Oversight bodies are responsible for the strategic direction of the organization and ensuring the proper implementation and design of internal controls, such as cybersecurity controls.

PricewaterhouseCoopers, speaking about governing boards for private companies, says that boards need to 1) embed cyber risk in strategic decisions, 2) understand the cyber risk management program, and 3) monitor cyber resilience.

When cybersecurity briefings do occur, they are typically triggered as needs arise rather than being part of a structured process. This lack of intentional communication is concerning as cyber threats continue to grow and evolve.

Involving governing bodies and keeping them informed on cybersecurity can be done effectively. One drinking water system with strong cybersecurity controls told us the following about the relationship with its governing body:

Utah Drinking Water System

"Annually I will give our [governing body] an update/presentation on our current cyber security risk and position. I will show them recent threats that we're seeing and give an update on what our department is doing and measures we take to further secure our infrastructure. Our [governing body] is proactive and will ask direct questions to me throughout the year of cyber related issues they may see in their other assignments…."

Getting governance right is key to organizational success. Our office published *The Best Practice Handbook*,[8] which states:

The Best Practice Handbook

"Effective governance broadly establishes the structures and processes necessary to direct, inform, manage, and monitor an organization. When the governing body applies principles of good governance, it fosters organizational success and augments the value the organization provides."

The Best Practice Handbook details principles of good governance. Three are relevant here: active and invested governance body; effective interaction with the board, management, and auditors; and clear definition and implementation of risk management policies. Infrequent cybersecurity briefings to governing bodies and the absence of strategic planning go against these principles.

The pathway to improving drinking water cybersecurity relies on improving governance and the practices of governing bodies. Water systems frequently cited insufficient staffing and resources as barriers to improving cybersecurity. Drinking water governing bodies could potentially address these constraints in several ways. They could 1) generate additional revenue, 2) reallocate existing resources, or 3) use existing resources provided by the federal and state governments more extensively.

The pathway to improving drinking water cybersecurity relies on improving governance and the practices of governing bodies.

Based on the findings in this chapter and the potential consequences of cyberattacks, we recommend that community water systems adopt best practices consistent with EPA

[8] Utah Office of the Legislative Auditor General. *The Best Practice Handbook*. Report No. 2023-05, May 2023.

guidance. The Utah Drinking Water Board has the authority to develop administrative rules "…governing the design, construction, operation, and maintenance of public water systems."[9] However, the board has not adopted any rules on cybersecurity for drinking water systems and many water systems do not have multi-year plans to improve cybersecurity. The board should require all community water systems that use OT to develop a plan to improve cybersecurity by implementing baseline best practices.

RECOMMENDATION 1.1

The Utah Drinking Water Board should require all community water systems that use operational technology to adopt a plan to implement cybersecurity best practices like those outlined by the U.S. Environmental Protection Agency. Plans should target baseline best practices to provide a solid foundation for cybersecurity.

This recommendation gives flexibility to 1) the Utah Drinking Water Board to determine which best practices should be implemented and 2) drinking water systems to determine how to implement best practices. Given the risk to drinking water systems, the Legislature should consider whether any additional steps should be taken to further address the cybersecurity risk to drinking water systems.

RECOMMENDATION 1.2

The Legislature should consider whether any additional steps should be taken to further address cybersecurity risk to drinking water systems.

Governing bodies need to ensure they are adequately addressing cybersecurity risk. A governing body cannot provide oversight over cybersecurity efforts if it is not told the cyber risk and possible responses to that risk. It's unclear whether the Utah Drinking Water Board can place governance requirements on governing bodies that oversee drinking water systems. The Legislature should consider requiring that bodies that govern drinking water systems be regularly briefed on cybersecurity.

[9] ***Utah Code*** 19-4-104.

RECOMMENDATION 1.3

The Legislature should consider modifying statute to require drinking water systems that have governing bodies to provide regular cybersecurity briefings to their governing council or board. Briefings should include information on existing protections, cybersecurity risk, and the results of any cybersecurity assessments completed.

We believe improved governance, including a more strategic approach to cybersecurity, will help elevate cybersecurity at Utah's water systems.

Complete List of Audit Recommendations

Complete List of Audit Recommendations

This report made the following three recommendations. The numbering convention assigned to each recommendation consists of its chapter followed by a period and recommendation number within that chapter.

Recommendation 1.1

The Utah Drinking Water Board should require all community water systems that use operational technology to adopt a plan to implement cybersecurity best practices like those outlined by the U.S. Environmental Protection Agency. Plans should target baseline best practices to provide a solid foundation for cybersecurity.

Recommendation 1.2

The Legislature should consider whether any additional steps should be taken to further address cybersecurity risk to drinking water systems.

Recommendation 1.3

The Legislature should consider modifying statute to require drinking water systems that have governing bodies to provide regular cybersecurity briefings to their governing council or board. Briefings should include information on existing protections, cybersecurity risk, and the results of any cybersecurity assessments completed.

Agency Response Plan

State of Utah

SPENCER J. COX
Governor

DEIDRE HENDERSON
Lieutenant Governor

Department of
Environmental Quality

Tim Davis
Executive Director

Ashley Sumner
Deputy Director

Jill Burton
Deputy Director

January 23, 2026

Kade R. Minchey, CIA, CFE, Auditor General
Office of the Legislative Auditor General
Utah State Capitol Complex
Rebecca Lockhart House Building, Suite W315
PO Box 145315
Salt Lake City, UT 84114-5315

Dear Mr. Minchey,

Thank you for the opportunity to respond to the recommendations in *A Performance Audit of Drinking Water Cybersecurity (2026-01)*. We appreciate the effort and professionalism of you and your staff in this review, as well as your willingness to communicate with the Department of Environmental Quality team throughout the audit process.

We concur with all recommendations in this report and have outlined the plan of action to address each recommendation below. Our teams in the Department of Environmental Quality are ready to take action, partner on actions, and assist the Legislature in their decisions to enhance cybersecurity for Utah's public drinking water systems.

The Department of Environmental Quality is committed to efficient operational processes and effective use of taxpayer funds and values the insight this report provides on areas that need improvement.

Sincerely,

Tim Davis (Jan 23, 2026 10:50:56 MST)
Tim Davis, Executive Director

TD/blj

195 North 1950 West • Salt Lake City, UT
Mailing Address: PO Box 144810 • Salt Lake City, UT 84114-4810
Telephone (801) 536-0095
www.deq.utah.gov

Recommendation 1.1: The Utah Drinking Water Board should require all community water systems that use operational technology to adopt a plan to implement cybersecurity best practices like those outlined by the U.S. Environmental Protection Agency. Plans should target baseline best practices to provide a solid foundation for cybersecurity.
Department Response: The department concurs.

What: The Division of Drinking Water teams will work with the Utah Drinking Water Board and legislators to establish statutes, rules, and policy requirements to better align cybersecurity best practices with those of the U.S. Environmental Protection Agency.

How: The Division of Drinking Water will assist legislators in developing cybersecurity legislation and initiate a parallel rulemaking process with the Drinking Water Board to ensure the new statute is fully addressed.

Legislation and rulemaking will require all community public water systems to complete an emergency response plan that includes cybersecurity best management practices, including requirements to:

- Support and regularly update the software used in a control system
- Deploy and maintain network protection for a control system, as needed
- Adopt best practices for secure authentication
- Provide annual cybersecurity training to an employee who has regular access to an operational technology or control system
- Complete an internal assessment of the community water system's security vulnerabilities and implement corrective controls to address the security vulnerability
- Promptly remove access to all operational technology and control systems from an employee whose employment is terminated
- Prohibit the unauthorized copying of software and data
- Ensure that an automated operational technology or control system can be operated manually, as needed
- Report a security breach in accordance within timeframes established by the legislature
- Adopt other security and records management requirements in conformity with state and federal requirements
- Comply with a security directive by the Division of Drinking Water director

When: The Department will assist legislators during the 2026 Legislative session in advancing statutes to require cybersecurity best management practices in emergency response plans for all community public drinking water systems. A supplier of a community water system serving a population of 3,300 or greater shall complete an emergency response plan by no later than December 31, 2026, and July 1 annually thereafter. A supplier of a community water system serving a population of less than 3,300 shall complete an emergency response plan by no later than July 1, 2027, and annually thereafter.

Contact: Nathan Lunstad, PhD, PE, Director, Division of Drinking Water, nlunstad@utah.gov, 385-239-5974

Recommendation 1.2: The Legislature should consider whether any additional steps should be taken to further address cybersecurity risk to drinking water systems.

Department Response: The Department of Environmental Quality will support the Legislature as it considers additional steps to address cybersecurity. If legislative changes occur, the Department of Environmental Quality will align its Administrative Rules, policies, and procedures to this new direction.

What: The Department will conduct an assessment of areas where further legislation may be effective in addressing cybersecurity risk for drinking water systems. Areas for assessment will include integrating cybersecurity into sanitary surveys, reporting and information sharing requirements, cybersecurity CEUs for operator certification and training, and funding needs for cybersecurity planning and infrastructure improvements.

When: The Department will complete this assessment by December 31, 2026.

Contact: Nathan Lunstad, PhD, PE, Director, Division of Drinking Water, nlunstad@utah.gov, 385-239-5974

Recommendation 1.3: The Legislature should consider modifying statute to require drinking water systems that have governing bodies to provide regular cybersecurity briefings to their governing council or board. Briefings should include information on existing protections, cybersecurity risk, and the results of any cybersecurity assessments completed.

Department Response: The Department of Environmental Quality will support the Legislature as it considers drinking water systems that have governing bodies to provide regular cybersecurity briefings to their governing council or board. If legislative changes occur, the Department of Environmental Quality will align its Administrative Rules, policies, and procedures to this new direction.

What: The Department will develop a guide for water systems for effective cybersecurity briefings to their governing bodies. This framework will help ensure water systems are clearly communicating risk and budgetary needs to strategic decision makers, and will establish briefings as a best practice in anticipation of legislation.

When: The Department will develop a cybersecurity briefing guide for drinking water systems by December 31, 2026.

Contact: Nathan Lunstad, PhD, PE, Director, Division of Drinking Water, nlunstad@utah.gov, 385-239-597415

THE MISSION OF THE LEGISLATIVE AUDITOR GENERAL IS TO

AUDIT · LEAD · ACHIEVE

WE HELP ORGANIZATIONS IMPROVE

olag.utah.gov