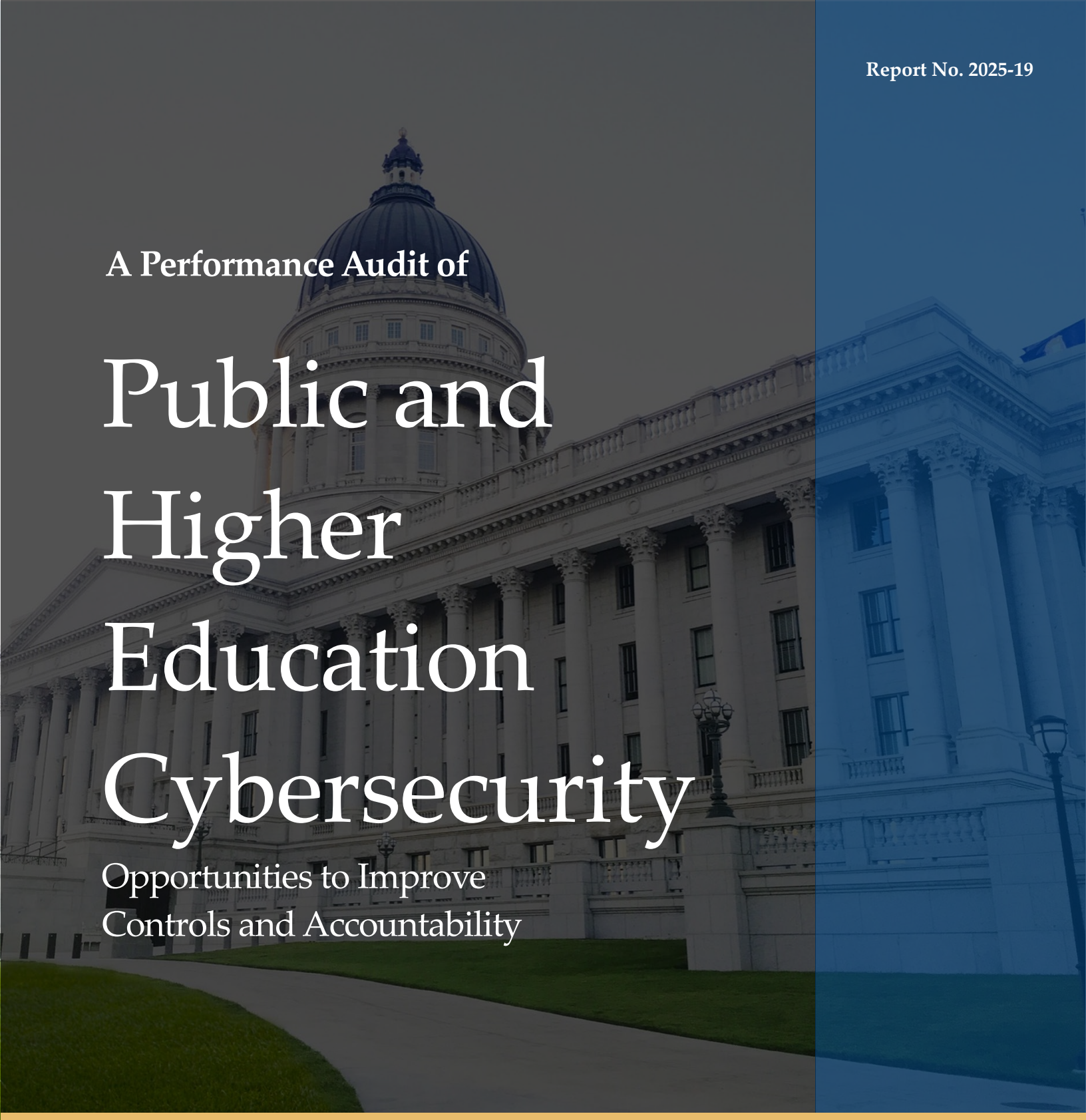
Report No. 2025-19



A Performance Audit of

Public and Higher Education Cybersecurity

Opportunities to Improve Controls and Accountability

Office of the Legislative Auditor General

Report to the **UTAH LEGISLATURE**

LEGISLATIVE AUDITOR GENERAL
1975 - 2025


LEGISLATIVE AUDITOR GENERAL
50
1975 - 2025

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

W315 House Building State Capitol Complex | 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

September 25, 2025

TO: THE UTAH STATE LEGISLATURE

Transmitted herewith is our report:

"A Performance Audit of Public and Higher Education Cybersecurity" [Report #2025-19].

An audit summary is found at the front of the report. The scope and objectives of the audit are included in the audit summary. In addition, each chapter has a corresponding chapter summary found at its beginning.

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 Board of Higher Education is Amanda Covington. Amanda Covington 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 2025-19 | SEPTEMBER 2025

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

PERFORMANCE AUDIT

EDUCATION CYBERSECURITY

KEY FINDINGS

- **1.1** Local education agencies can do more to meet baseline cybersecurity best practices.
- **2.1** Higher education has complex systems and sensitive data that require stronger oversight.
- **2.2** Additional validation may be needed for cybersecurity controls on future audits.

RECOMMENDATIONS

- **1.1** The Legislature should consider studying minimum cybersecurity standards for local education agencies. These minimum standards could follow the principles behind high-priority practices outlined by the Cybersecurity & Infrastructure Security Agency that are 1) attainable by local education agencies, regardless of size and 2) proven to reduce risk.
- **2.1** The Utah Board of Higher Education should clarify roles, including accountability for compliance, for the Utah System of Higher Education and its member institutions in the cybersecurity policy. The policy should define the purpose of the policy and how information security plans and programs are to be used. The purpose of these changes is to ensure decisions are made according to sound information and institutions are held accountable for cybersecurity.
- **2.2** The Legislative Audit Subcommittee should consider including cybersecurity testing and validation as part of current and future audits done by the Office of the Legislative Auditor General. This will enable a broader assessment of government agency performance and effectiveness and ensure emerging risks are addressed.

AUDIT REQUEST

The Legislative Audit Subcommittee prioritized an audit of cybersecurity readiness throughout the state, including public and higher education, in its October 2024 meeting.

BACKGROUND

Cybersecurity threats such as ransomware, data breaches, and corporate email fraud are increasing in public education. Recent incidents in Utah have resulted in financial losses and exposed student data. Cyber attacks in other states demonstrate the possibility of consequences on an even larger scale in both public and higher education.

Public schools and higher education institutions can look to best practices to prioritize and implement cybersecurity controls. These practices are essential to protecting sensitive information and preventing financial losses.

REPORT SUMMARY

Local Education Agencies Are Falling Short of Essential Cybersecurity Best Practices

Utah's local education agencies (LEAs) are not fully implementing baseline cybersecurity practices, leaving school systems vulnerable. Recent attacks in Utah exposed data from hundreds of thousands of students and employees and cost districts over $150,000. Testing and statewide surveys found significant gaps in incident response planning, training, and patch management, with smaller districts lagging furthest behind. Barriers such as insufficient staffing, limited resources, and lack of prioritization continue to hinder progress. The Legislature can help drive improvement by studying possible minimum cybersecurity standards and solutions to LEAs' cybersecurity challenges.

Higher Education Can Do More to Improve Cybersecurity Controls and Cybersecurity Governance

Utah's higher education institutions have largely adopted high-impact practices but vary widely in their implementation of a broader set of cybersecurity controls. Weaknesses are most evident in web and email safeguards and in cybersecurity training, both critical areas exploited by attackers. Oversight and accountability are also inconsistent, as institutions differ in how they develop and communicate information security plans. The Utah Board of Higher Education can better define roles and responsibilities within higher education. Stronger governance and more consistent baseline protections would help protect sensitive student, financial, and research data.

Survey Data Points to Gaps in Key Cybersecurity Practices in LEAs

Using survey data from the Utah Education and Telehealth Network, we found gaps in the execution of key cybersecurity best practices. A large number of LEAs fell behind in key areas such as implementation of multifactor authentication, incident response plans, training, and patch management.

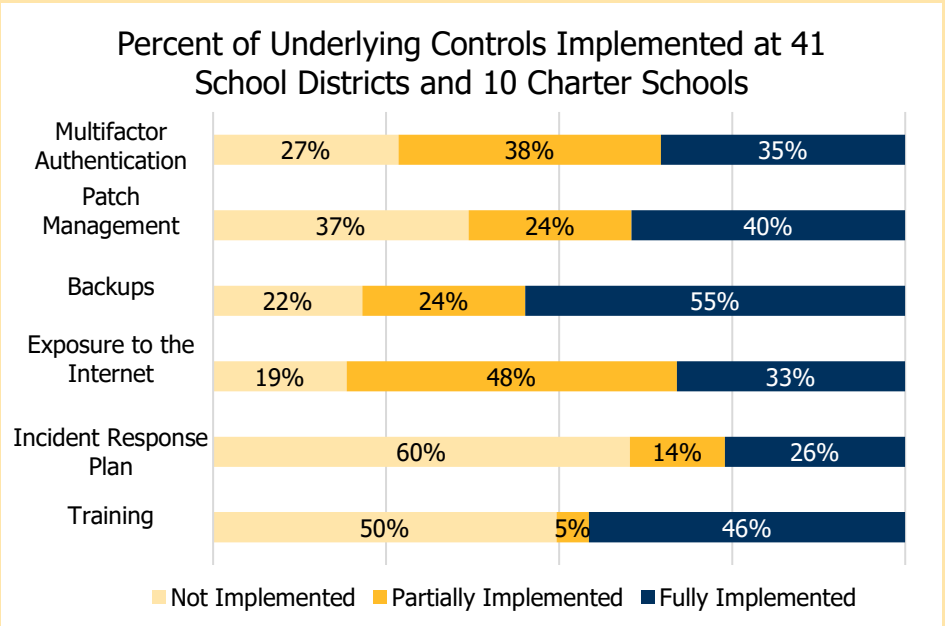


Table of Contents

CHAPTER 1 Summary

Local Education Agencies Are Falling Short of Essential Cybersecurity Best Practices

BACKGROUND

Cybersecurity threats like ransomware, data breaches, and corporate email fraud are increasing in public education. Successful cyber attacks can lead to significant financial losses, loss of trust, and a disruption of education. Attackers successfully struck two Utah school districts recently leading to financial losses and breached student data. Best practices published by government agencies provide guidance to local education agencies (LEA) on how to prioritize cybersecurity controls.

FINDING 1.1
Local Education Agencies Can Do More to Meet Baseline Cybersecurity Best Practices

RECOMMENDATION 1.1

The Legislature should consider studying minimum cybersecurity standards for local education agencies. These minimum standards could follow the principles behind high-priority practices outlined by the Cybersecurity & Infrastructure Security Agency that are 1) attainable by local education agencies, regardless of size and 2) proven to reduce risk.

RECOMMENDATION 1.2

The Legislature should consider studying possible solutions to challenges faced by Utah local education agencies like insufficient prioritization of cybersecurity, staffing, training, and recruiting and retaining skilled personnel. If the Legislature studies this issue, it should consider the differences between large and small school districts in implementing cybersecurity controls.

CONCLUSION

Based on testing results and survey data, Utah LEAs are not fully implementing foundational cybersecurity practices. In addition, small school districts appear to be fully implementing fewer cybersecurity controls than large school districts. Gaps in cybersecurity put LEAs at risk for successful cyber attacks. LEAs told us that they face challenges in improving cybersecurity including staffing, insufficient prioritization of cybersecurity, and insufficient training. The Legislature can take steps to help LEAs prioritize cyber controls by studying minimum cybersecurity standards. Ongoing work may be needed to validate the implementation of cybersecurity controls on future audits.

Chapter 1
Local Education Agencies Are Falling Short of Essential Cybersecurity Best Practices

Public education can do more to address the many cybersecurity threats it faces. These threats include ransomware, data breaches, and corporate email fraud that can lead to significant financial losses, loss of trust, and a disruption of education. Meanwhile, addressing cybersecurity threats can be difficult because it is an evolving landscape. We found that local education agencies (LEAs) can be more aggressive in defending against these threats. Providing additional guidance to LEAs on the most important cybersecurity controls may be part of the solution. Survey results from education cybersecurity experts indicate that LEAs are insufficiently prioritizing cybersecurity and may not know what controls they should be implementing. The Legislature can help drive improvement by studying possible minimum cybersecurity standards and solutions to LEAs' cybersecurity challenges.

1.1 Local Education Agencies Can Do More to Meet Baseline Cybersecurity Best Practices

Cybersecurity testing and survey results show that LEAs in Utah can do more to implement foundational cybersecurity practices. Gaps in cybersecurity controls can lead to financial loss and identity fraud. These weaknesses could be due to LEAs insufficiently prioritizing cybersecurity for things like staffing. Thus, the Legislature should consider studying possible minimum cybersecurity standards for LEAs. The Legislature should also consider studying how to address persistent barriers to LEA cybersecurity, such as low prioritization of cybersecurity, inadequate staffing, and challenges in training and retaining skilled personnel.

The number of cyber attacks on public education is increasing, and the cost of these attacks can be significant.

LEAs Face Significant Consequences from Successful Cyber Attacks

The number of cyber attacks on public education is increasing, and the cost of these attacks can be significant. Successful Utah attacks have cost districts financially and in staff time and impacted hundreds of thousands of students and employees. Cyber attacks have also significantly impacted school districts in other states.

Recent Attacks Impacting Utah LEAs Have Led to Breached Data and Financial Costs. These attacks occurred in two Utah school districts and at a vendor that provides services to many school districts in the state.

According to the first school district, an attacker was able to infiltrate their system and begin stealing data. While the district was able to detect and limit the damage of the attack, it still impacted the data for approximately 450,000 students and 30,000 employees. Breaches of education data can result in a violation of the U.S. Family Educational Rights and Privacy Act and can lead to identity theft, fraud, and extortion of students. The school district paid $150,000 to their cyber insurance provider and dedicated significant amounts of technical staff time to recovery. The district reported that 7 full-time equivalent employees spent about 75 percent of their time over 4 to 5 months to recover from the attack. This is significant because LEAs told us that staffing is a barrier to improving cybersecurity. Instead of improving cybersecurity controls, this district was forced to respond to an attack.

Utah School District #1

Data for 450,000 Students and 30,000 Employees Impacted

$150,000 Insurance Deductible Paid

Attackers successfully struck a separate Utah school district in the last year with a total estimated cost between $100,000 and $150,000. This included payments to their insurance provider and overtime to district employees. The attack occurred right before spring break, so the impact was likely less than it could have been.

Paid Between $100,000 and $150,000 in Insurance Premiums and Overtime Costs

Occurred Before Spring Break, Mitigating the Impact

Utah School District #2

Notably, the attacks on both school districts could have been prevented by more fully implementing multifactor authentication (MFA), a best practice discussed later in this chapter. In addition to the two school districts, an education software vendor reported a breach in 2024 that affected the data of customer LEAs in Utah. It may have been the largest breach of personal information for students nationwide. Attackers were able to access systems because MFA was not enabled on a compromised employee account.

Cyber Attacks Are Impacting Public Education in Other States. According to the U.S. Government Accountability Office, the number of reported cyber incidents in public education in the United States grew from 400 in 2018 to 1,300 in 2021. Cyber attacks in public education around the United States have been widely reported by government agencies and news organizations.

As part of a ransomware attack in 2021, an attacker disclosed personal information for over 500,000 students and employees associated with Chicago Public Schools.

The following attacks occurred in Texas schools in 2020: seven ransomware attacks, three denial-of-service attacks, two data breaches, and one phishing incident. One district paid a $500,000 ransom, and one district experienced a denial-of-service attack on the first day of classes.

One school district in Connecticut had to shut down for 3-4 days due to a cybersecurity incident. One district in the state initially lost more than $6 million after a cyber attack.

Broward County Public Schools suffered a ransomware attack that led to a breach of nearly 49,000 records. Miami-Dade County School District was a target of more than twelve denial-of-service attacks as students returned to school in fall 2020.

Coventry Public Schools fell victim to a ransomware attack that led to a ransom payment of $300,000. The attack shut down the HVAC system which allowed black mold to spread in their facilities.

Baltimore County Public Schools suffered an attack in 2020 that led to the cancelation of classes for three days. It took the district over a year to fully recover from the attack.

Albuquerque Public Schools shut down for two days as they recovered from a ransomware attack. The district paid a forensics company $250,000 to analyze the attack.

Source: U.S Government Accountability Office, multiple news organizations, Comparitech, Govtech, and The School Superintendents Association.

Cyber attacks have had real impacts on school districts in Utah. Additionally, attacks in other states demonstrate potentially significant impacts that Utah LEAs could experience during future cyber attacks.

Federal Agencies and Cybersecurity Experts Have Prioritized Best Practices for LEAs

The federal government has developed cybersecurity best practices that are applicable to organizations, even those that are small. The Cybersecurity & Infrastructure Security Agency (CISA)[1] worked with experts and various industries to develop Cross-Sector Cybersecurity Performance Goals which provide a minimum baseline of cybersecurity practices for organizations regardless of industry. CISA also prioritized these practices for public education entities. Recognizing that cybersecurity is not one-size-fits-all and resources are finite, CISA's prioritized practices provide a starting point that LEAs can pursue. These practices are listed and explained in the following infographic.

Source: Protecting Our Future: Partnering to Safeguard K-12 Organizations From Cybersecurity Threats.

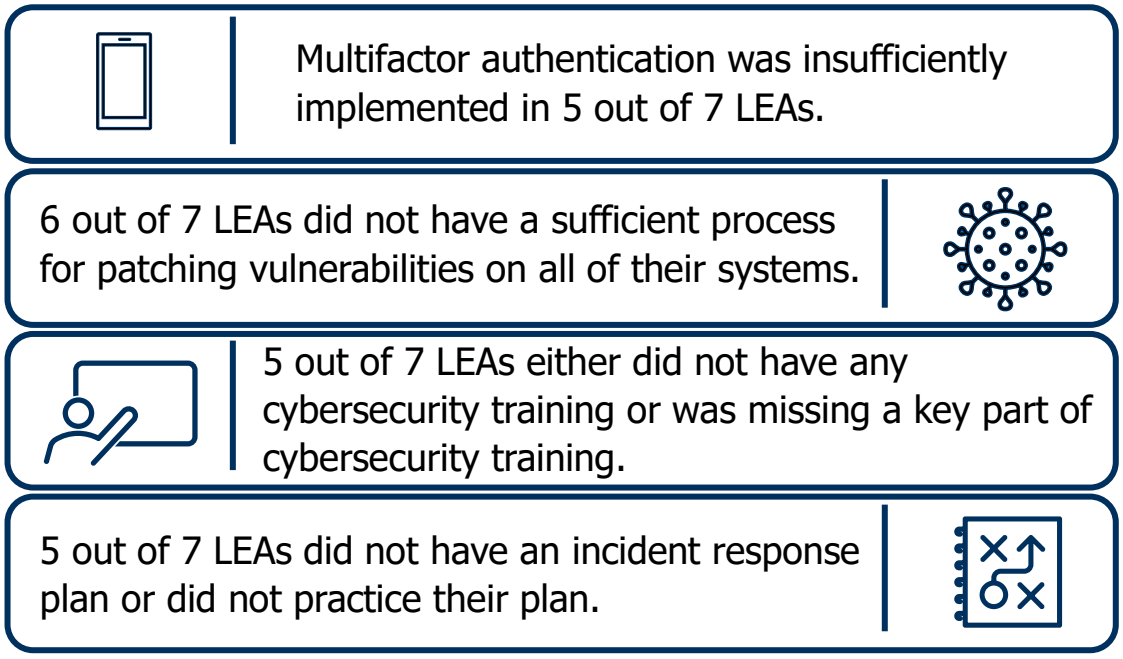
[1] The Cybersecurity & Infrastructure Security Agency is part of the U.S. Department of Homeland Security and coordinates efforts to protect critical infrastructure.

These priority practices have been proven to reduce the risk of cyber attacks and are informed by actual threats. Thus, we used these six beneficial practices to guide our testing of LEAs.

Testing and Survey Data Show Important Gaps in Key Cybersecurity Controls

As part of this audit, we used CISA's six high-priority practices (as shown on the previous page) to guide testing of a sample of LEAs. We also analyzed statewide survey data gathered at the direction of the Utah Education and Telehealth Network (UETN). Both the testing conducted by the state of Utah's Division of Technology Services (DTS) and UETN's survey data point out gaps in the use of baseline cybersecurity controls. It also appears that large school districts have more robust cybersecurity protection than small school districts.[2]

DTS Tested the Adequacy of Priority Practices in a Sample of LEAs and Found Gaps. This sample included six school districts and one charter school of various enrollment sizes.[3] The testing found the following:



Source: Division of Technology Services testing data of seven local education agencies and survey questions administered by the Office of the Legislative Auditor General.

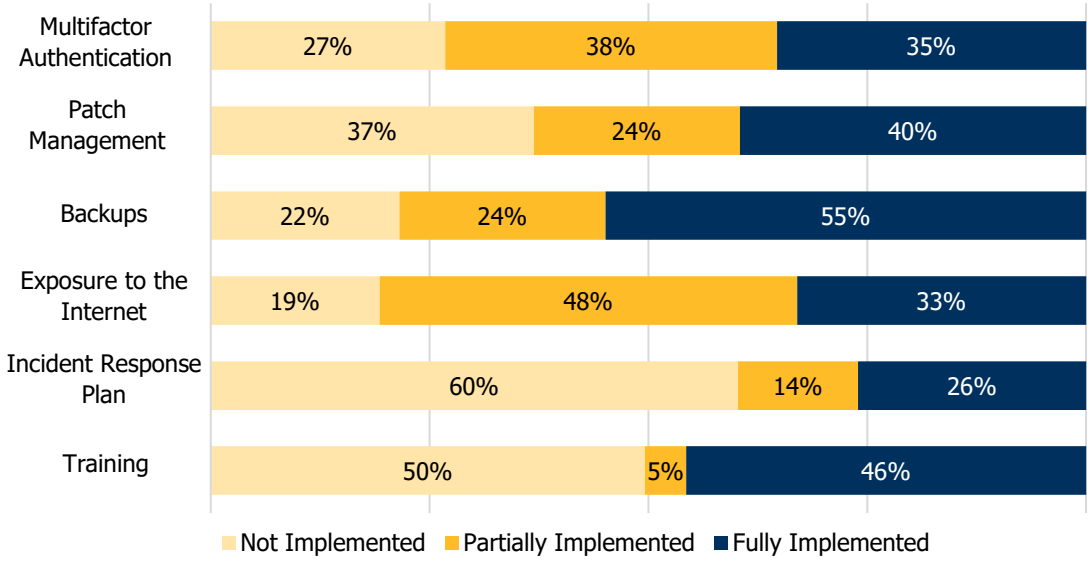
[2] We defined large school districts as school districts at or above the median October 1, 2024, enrollment. Small school districts are those below the median October 1, 2024, enrollment.

[3] The next section summarizes statewide survey data for a larger set of LEAs.

These gaps cover four of the six high-priority practices identified by CISA, meaning more than half of the seven tested LEAs are insufficiently implementing certain baseline controls. The seven tested LEAs generally appear to do better on reducing exposure to the internet and backing up servers.

UETN's Survey Data Also Identified Gaps in Priority Cybersecurity Practices. This survey asked over 400 questions to representatives at 41 school districts and a sample of 10 charter schools. Responses to these questions were used to determine the implementation status of 88 cybersecurity controls.[4] We looked at the implementation status of all controls that relate to CISA's six high-priority practices. Figure 1.1 shows the implementation status for all LEAs surveyed for relevant cybersecurity controls.

Figure 1.1 Survey Data Points to Gaps in Key Cybersecurity Practices in LEAs. Incident response plans and training are the two practices for which the highest percentage of cybersecurity controls were not implemented among LEAs. All school districts and ten charter schools are represented in this data.*

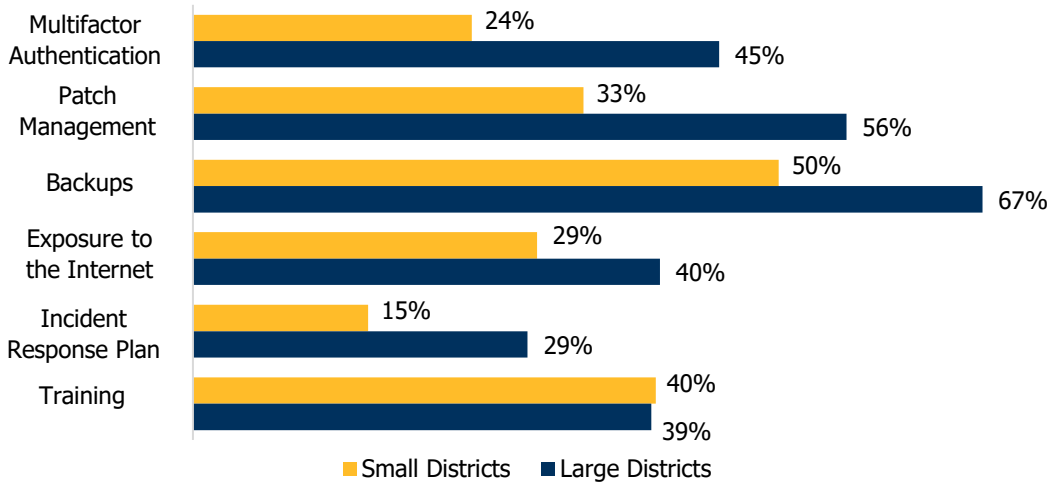


Source: Utah Education and Telehealth Network cybersecurity survey data.
**Data is for 41 school districts and 10 charter schools and was generated by a vendor on behalf of the Utah Education and Telehealth Network.*

Looking at just the fully implemented controls, large school districts appear to be better protected. Figure 1.2 divides all 41 school districts into large and small districts and looks at the percentage of underlying controls fully implemented.

[4] The list of 88 cybersecurity controls is a subset of those found in the Center for Internet Security (CIS) Critical Security Controls and includes all CIS essential cyber hygiene controls.

Figure 1.2 Survey Data Indicates Large School Districts Are Better Positioned Against Cyber Attacks. With the exception of training, large school districts appear to be farther along than small school districts in implementing CISA's high-impact practices.*



Source: Utah Education and Telehealth Network cybersecurity survey data.
**Data is for 41 school districts and was generated by a vendor on behalf of the Utah Education and Telehealth Network.*

These figures, along with testing data from DTS, demonstrate 1) that LEAs are not fully implementing baseline cybersecurity practices and 2) small school districts have larger gaps in cybersecurity controls. This puts LEAs, especially small ones, at risk for successful cybersecurity attacks.

The gaps in LEAs' cybersecurity practices are important. For example, MFA is critical because it provides an additional barrier to attackers accessing important systems and data. Increasingly, attackers can get passwords by cracking or guessing them, phishing for them through email, or identifying passwords used on other systems. The two cyber attacks in Utah LEAs and the attack on a major vendor discussed earlier could have been prevented by implementing MFA.

In addition, many cyber attacks are successful because computer software has not been updated to newer versions. According to CISA, "Keeping systems patched is one of the most cost-effective practices an organization can adopt to enhance its security posture."[5] Training is important because many cybersecurity breaches are the result of human error. Effective training prepares employees to be able to both identify threats and develop good habits. While some of these precautions seem straightforward, LEAs face barriers to implementing cybersecurity controls.

[5] Sophos, a cybersecurity company, reported that 44 percent of ransomware attacks in public education were caused by exploited vulnerabilities in 2024. Compromised credentials were the cause of 20 percent of ransomware attacks in the same year.

LEAs Face a Variety of Barriers to Implementing Cybersecurity Controls

As part of this audit, our team sent a survey to over 140 information security officers in every LEA in the state. This survey was separate from UETN's but provided context for several of the UETN survey's results. We asked LEAs about the three biggest barriers they face in implementing cybersecurity controls.[6] Figure 1.2 shows the top challenges LEAs report facing in implementing cybersecurity controls, besides funding.

Figure 1.2 The Results of Our LEA Survey Revealed Staffing to Be the Biggest Barrier to Implementing Cybersecurity Controls. Several of these challenges could be addressed by LEAs making cybersecurity a higher priority.

Source: Office of the Legislative Auditor General survey data.
Note: Of the over 140 individuals who received the survey, 58 individuals answered this question. The data is represented as reported to us for the nine most frequently selected barriers. We were unable to follow-up with LEAs because the survey was anonymous.

LEAs are ultimately responsible for protecting themselves from cyber attacks. However, the state could play a role in addressing some of the challenges that LEAs face. For example, House Bill 40 became law after the 2025 General Session of the Utah State Legislature. This bill requires that the School Security Task Force "…study possible recommendations for minimum cybersecurity standards for

LEAs are ultimately responsible for protecting themselves from cyber attacks. However, the state could play a role in addressing some of the challenges that LEAs face.

[6] We received about 62 responses to our survey, distributed between school districts and charter schools, small LEAs and large LEAs

local education agencies."[7] However, the School Security Task Force is only authorized through the end of December 2025. Minimum standards could address LEA concerns on prioritizing cybersecurity controls. Earlier in this chapter, we discussed CISA's high-priority practices for cybersecurity in public education. The Legislature should consider studying minimum cyber standards for public education, such as CISA's high-priority practices, to help provide a foundation for LEAs to build upon. As previously stated, CISA's six practices are proven to reduce cybersecurity risk and counter known threats.

RECOMMENDATION 1.1

The Legislature should consider studying minimum cybersecurity standards for local education agencies. These minimum standards could follow the principles behind high-priority practices outlined by the Cybersecurity & Infrastructure Security Agency that are 1) attainable by local education agencies, regardless of size and 2) proven to reduce risk.

The Legislature could also study possible solutions to difficult challenges faced by LEAs. We believe staffing, recruiting, training, and governance challenges could be addressed at the LEA level. UETN and the Utah State Board of Education are already attempting to address the challenge of insufficient cooperative contracts. However, survey data indicates all of these challenges, especially staffing, are pervasive across LEAs. We have found little evidence of surrounding states[8] directly addressing the cybersecurity challenges expressed by Utah's LEAs. The Legislature should consider studying possible solutions to challenges faced by Utah LEAs like insufficient prioritization of cybersecurity, staffing, training, and recruiting and retaining skilled personnel. If the Legislature studies this issue, it should take into account the differences between large and small school districts in cybersecurity capabilities.

We believe staffing, recruiting, training, and governance challenges could be addressed at the LEA level. However, survey data indicates all of these challenges, especially staffing, are pervasive across LEAs.

[7] The Legislature created the School Security Task Force in 2023 to address safety and security in Utah's public schools. It has 19 members from across state government including 4 legislators.

[8] Arizona does have a program where school districts can submit an application requesting licenses for things like firewalls, training, and MFA.

RECOMMENDATION 1.2

The Legislature should consider studying possible solutions to challenges faced by Utah local education agencies like insufficient prioritization of cybersecurity, staffing, training, and recruiting and retaining skilled personnel. If the Legislature studies this issue, it should consider the differences between large and small school districts in implementing cybersecurity controls.

As stated previously, cyber attacks are growing in public education and costs associated with successful attacks can be significant. This indicates that the need for additional assessments and validation of cybersecurity will continue to be relevant. At the end of Chapter 2 of this report, we make a recommendation to the Legislature to increase the state's capacity to assess cybersecurity controls in areas audited by the Office of the Legislative Auditor General.

BACKGROUND

Cybersecurity threats facing higher education are becoming increasingly sophisticated, putting Utah's colleges and universities at risk. The Utah System of Higher Education (USHE) includes institutions serving more than 200,000 students statewide, each operating complex IT systems that are attractive targets for cyber attacks. Recent incidents in Utah and across the nation, including ransomware attacks, data breaches, and other compromises, have demonstrated the significant financial and operational consequences such events can have on higher education.

FINDING 2.1
Higher Education Has Complex Systems and Sensitive Data That Require Stronger Oversight

RECOMMENDATION 2.1
The Utah Board of Higher Education should clarify roles, including accountability for compliance, for the Utah System of Higher Education and its member institutions in the cybersecurity policy. The policy should define the purpose of the policy and how information security plans and programs are to be used. The purpose of these changes is to ensure decisions are made according to sound information and institutions are held accountable for cybersecurity.

FINDING 2.2
Additional Validation May Be Needed for Cybersecurity Controls on Future Audits

RECOMMENDATION 2.2
The Legislative Audit Subcommittee should consider including cybersecurity testing and validation as part of current and future audits done by the Office of the Legislative Auditor General. This will enable a broader assessment of government agency performance and effectiveness and ensure emerging risks are addressed.

CONCLUSION

While USHE institutions are generally implementing the most critical cybersecurity practices, they vary significantly in their adoption of a broader set of baseline controls. Compliance with USHE board policy requiring a written information security plan informed by Center for Internet Security controls was also inconsistent, with several institutions either lacking a plan or having incomplete connections to a cybersecurity framework. The Utah Board of Higher Education should clarify roles and purpose in policy to improve accountability and decision making.

Chapter 2
Higher Education Can Do More to Improve Cybersecurity Controls and Cybersecurity Governance

Cybersecurity threats to colleges and universities are growing more sophisticated. Higher education institutions are targets because they hold student records, financial data, and intellectual property. These institutions serve over 200,000 students statewide and manage vast quantities of sensitive information. Utah System of Higher Education (USHE) institutions[9] appear to be implementing cybersecurity controls but can do more to ensure compliance and further progress in adopting baseline cybersecurity controls. Unaddressed weaknesses could expose the system to costly attacks.

2.1 Higher Education Has Complex Systems and Sensitive Data That Require Stronger Oversight

Institutions should ensure they are following Utah Board of Higher Education (board) policy and develop plans for implementing cybersecurity controls. These written plans should be informed by best practices adopted by the board. The board should ensure adequate oversight of cybersecurity at member institutions by clarifying policy. While USHE institutions have successfully implemented certain basic cybersecurity practices, more can be done to improve core cybersecurity controls and cybersecurity oversight within USHE.

Higher Education Cyber Attacks Can Be Costly Due to Large Amounts of Sensitive Information

Like public education, Utah's colleges and universities face a broad spectrum of cyber threats, including ransomware, business email fraud, and data breaches. However, these risks are elevated by more complex IT systems and additional sensitive data. USHE institutions and other higher education institutions around the country have been victims of cyber attacks.

USHE Institutions Face Cybersecurity Risks and Have Been Attacked. In 2020, the University of Utah's College of Social and Behavioral Science experienced a ransomware attack on its servers. The university paid a $457,000 ransom, most of which was reimbursed by their insurance provider. According to the university,

[9] This chapter focuses on the eight degree-granting institutions under the Utah System of Higher Education, not technical colleges, because degree-granting institutions make up a majority of student enrollment.

they paid a $60,000 insurance deductible and spent about 5,000 hours of staff time resolving the issue. USHE reports that a different institution had a data breach in 2021 where they had to notify about 3,800 people and had direct costs of $25,000. These incidents highlight actual cyber attacks that have occurred in Utah and their costs. Adopting the baseline cybersecurity practices discussed later in this chapter could have prevented the attacks on both institutions.

Nationwide Incidents Show That Higher Education Institutions Face Substantial Cybersecurity Risk. These incidents can involve breached data and ransomware.

The University of Maryland Global Campus reported a data breach affecting more than 300,000 students and staff including names, addresses, and Social Security numbers.

The physics and astronomy department at Michigan State University fell victim to a ransomware attack. Their research was halted, in some instances, for up to six months. Remediation costs were estimated at over $1 million.

University of California San Francisco suffered a ransomware attack on several servers. The university paid a ransom of over $1 million.

University of California Los Angeles Health suffered a breach of personal and health data that may have affected up to 4.5 million individuals.

The University of Colorado Boulder appears to have suffered multiple data breaches. The first involved 300,000 records with personal identifiable information. The second breach involved personal information for about 30,000 employees and students.

A cybersecurity incident at the University of Minnesota potentially affected the records of all individuals who applied to, attended, or worked for the university between 1989 and 2021.

In July 2023, Morehead State University took more than a month to recover from a ransomware attack. Only 20-21 people had their data breached, but the cost of recovery totaled about $1 million.

Source: University of California San Francisco, University of California Lost Angeles Health, Colorado Public Radio, University of Colorado Boulder, Indiana University, University of Minnesota, The HIPAA Journal, Morehead State University student newspaper, Comparitech.

Beyond ransom payments, it is estimated that downtime resulting from attack recovery can cost educational institutions about $548,185 per day on average. These examples show the consequences of actual cyber attacks in higher education. Although USHE institutions haven't experienced attacks of this size lately, the examples demonstrate the scale of possible future impacts on data breaches and expenses.

The Center for Internet Security Provides a Framework for Cybersecurity Protection in Higher Education

The Center for Internet Security (CIS) Critical Security Controls serve as the primary framework for evaluating cybersecurity across USHE institutions.[10] The CIS controls cover things like managing user accounts, inventorying assets, and data protection. Board policy requires its institutions to have a "…written information Security Plan and program informed by the CIS Critical Security Controls…."[11] Later in this chapter, we review data on the implementation of CIS controls by USHE institutions.

In Chapter 1 of this report, we discussed six high-impact cybersecurity practices identified by the Cybersecurity & Infrastructure Security Agency (CISA). This is a prioritized list of practices for public and higher education that covers things like multifactor authentication (MFA) and training.[12] Baseline CIS controls include these CISA practices but go further and include things like inventorying hardware and software assets.

Institutions are generally implementing the most important cybersecurity practices. However, there are areas for improvement in a broader group of baseline standards.

USHE Institutions Appear to Have Gaps in Baseline Cybersecurity Standards

Utah's higher education institutions are generally implementing the most important cybersecurity practices. However, according to a larger group of baselines standards, there are areas for improvement.

---

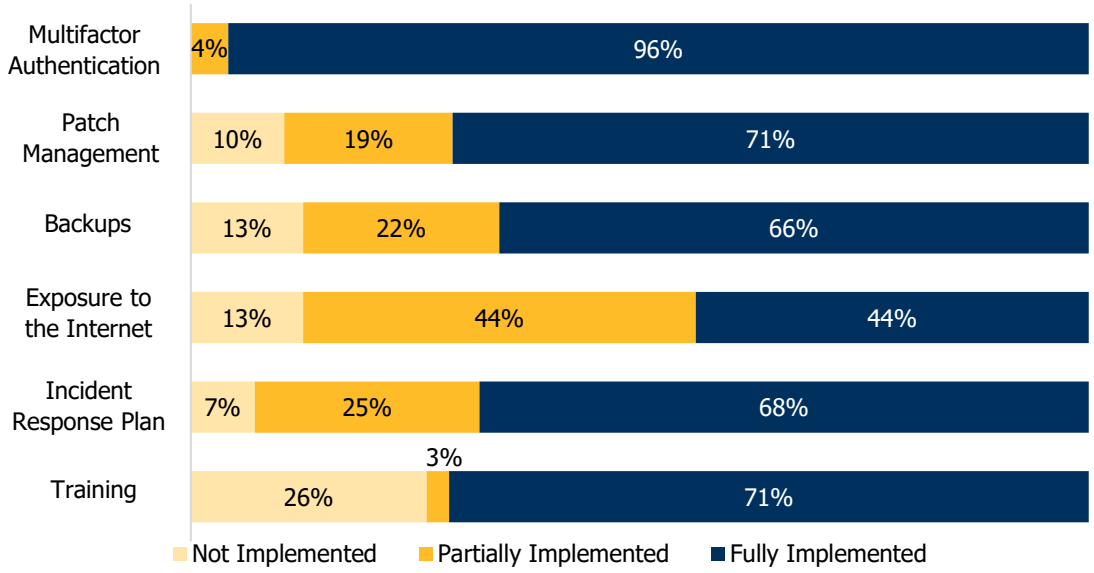
[10] CIS controls cover 18 categories of best practices designed to protect organizations from common threats. To make implementation more manageable, CIS categorizes organizations into three implementation groups based on resources, the organization's risks, and the complexity of the controls being implemented. The first implementation group is a baseline standard designed for organizations with IT and cybersecurity staff and focuses on basic cyber hygiene.

[11] Utah System of Higher Education Policy R345-4. Policy R345-3 defines a Security Plan as "…a formal document that provides an overview of the security requirements for an information system and describes the security controls in place or planned for meeting those requirements."

[12] CISA's practices are prioritized and are proven to reduce risk and address methods of attack.

USHE Institutions Are Generally Adopting the Six High-Priority Practices Used to Guide Our Testing of Local Education Agencies in Chapter 1 of This Report. Figure 2.1 shows the implementation status for CISA's six practices at all USHE institutions using survey data commissioned by the Utah Education and Telehealth Network (UETN).

Figure 2.1 A Survey From 2024 of All Degree-Granting Institutions Demonstrates They Are Generally Implementing High-Impact Cybersecurity Practices. Apart from reducing exposure to internet-based attacks, USHE institutions are implementing many controls underpinning CISA's high-impact practices.*



Source: Utah Education and Telehealth Network survey data.
**This represents the implementation status for the Center for Internet Security controls found in the survey data that underly CISA's high-impact practices.*

Crucially, USHE institutions are almost universally implementing MFA on their systems. The attacks on the University of Utah and another USHE institution, as well as the attacks on the two Utah school districts discussed in Chapter 1, demonstrate the importance of MFA.

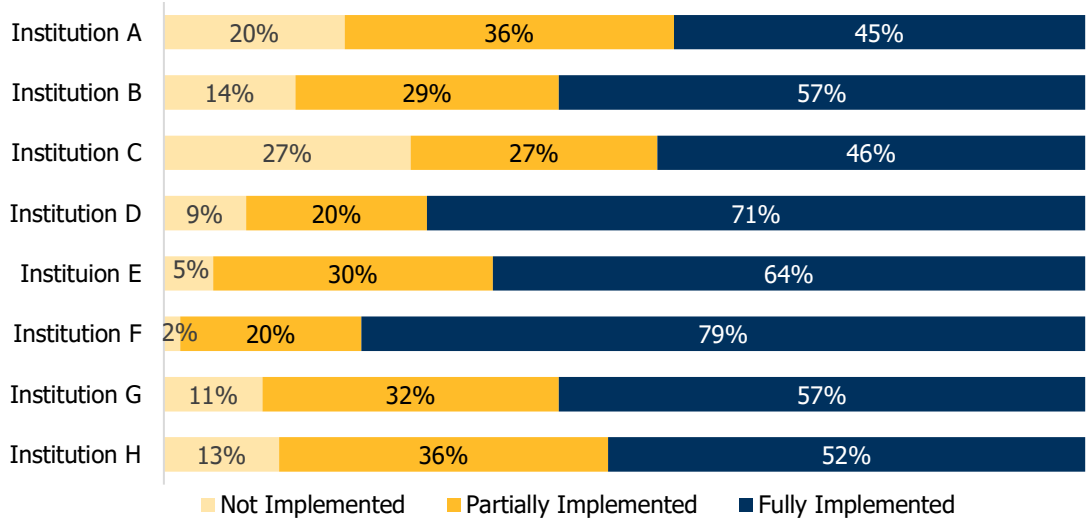
Crucially, USHE institutions are almost universally implementing MFA on their systems. MFA's importance is evident in attacks against the University of Utah, another USHE institution, and the two Utah school districts discussed in Chapter 1.

We are encouraged by the recurring cybersecurity assessments USHE institutions have been doing on each other for over a decade. Cybersecurity personnel from USHE institutions test the defenses of other institutions regularly. This shows good leadership and collaboration. It appears the thorough implementation of MFA may be the result of this institution collaboration. This also demonstrates how

positive outcomes can be achieved when institutions collaborate with each other.

Institutions Can Do More to Implement a More Expansive Set of Baseline Cybersecurity Controls According to the CIS Framework. Because USHE institutions generally do well in implementing CISA's high-priority practices, we also looked at all the baseline controls according to the CIS framework. These controls include the CISA practices found in Figure 2.1 as well as an expanded set of controls for things like hardware inventory and account management. We analyzed UETN survey data further by expanding the number of controls and breaking the data down by USHE institution. This determined institutional performance against a higher standard. When we drilled deeper, we found that institutions were less consistent in their implementation of this expanded set of controls. Figure 2.2 shows the status of baselines CIS controls for all eight degree-granting institutions.

Figure 2.2 USHE's Degree-Granting Institutions Vary in Their Implementation of a Wider Set of Cybersecurity Controls. Institutions vary from about 79 percent of baseline CIS controls implemented to about 45 percent.*



Source: Utah Education and Telehealth Network survey data.
**This represents the implementation status for all cyber hygiene controls also known as implementation group 1 Center for Internet Security safeguards.*

Institutions varied in their implementation of baseline CIS controls from 79 percent implemented at one institution to 45 percent at another. Utah's colleges and universities need to improve their cyber hygiene. Figure 2.2 shows incomplete implementation, potentially exposing systems to costly attacks.

Institutions have a low implementation rate for safeguards that protect web and email services.

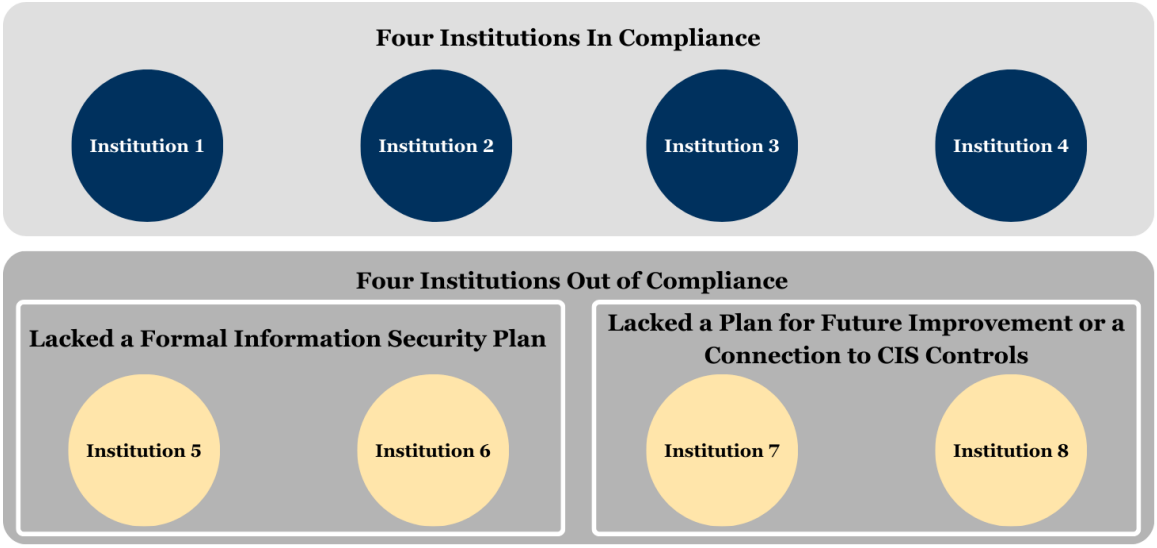
We believe the cybersecurity assessments done among USHE institutions have helped drive improvements. However, USHE's institutions have not yet implemented a number of

CIS's basic cyber hygiene controls. Overall, we found a low implementation rate for safeguards that protect web and email services across USHE institutions. Attackers often use websites and emails to trick people by interacting with them directly. Additionally, many institutions had not implemented safeguards related to cybersecurity awareness and skills training. Training arms employees with skills to be security conscious and reduce cybersecurity risks to the institution. It is vital that institutions follow best practices for cybersecurity training because attacks often arise from human error.

Institutions Could Benefit from Better Planning and Oversight

One thing that USHE institutions could do to improve their cybersecurity over time is to create a plan. As previously stated, USHE's board has a policy in place that requires member institutions to adopt and strive to implement CIS controls as a guiding security framework and the minimum institutional security standard. While institutions can create an individualized approach, policy stipulates that each institution should develop and maintain a written information security plan and program informed by these controls.

Institutions varied significantly in their compliance with this policy. Four institutions appear to be in compliance, and four appear to be lacking certain required elements.



Source: Office of the Legislative Auditor General communication with all eight degree-granting institutions.

How these plans inform decision-making and address cybersecurity risks also appear to vary. One institution told us they update their president through an informal process and update the audit committee of their board of trustees annually on cyber risk. Another institution stated their information security plan

goes through the risk committee but wasn't sure the institution's president was aware of cybersecurity risks. A third institution told us that the cybersecurity officer is on the institution's enterprise risk committee which includes multiple vice presidents. A previous audit stated that communication between cybersecurity experts and management often needs improvement.[13] Information security plans at USHE institutions can aid communication and drive informed decision making.

The Board Should Ensure Adequate Oversight of Cybersecurity

USHE's requirement for information security plans and programs is an initial step but does not ensure institutions are using these plans effectively or roles within USHE are clearly defined. Variation in policy compliance at institutions and unclear accountability likely contributed to the results in Figure 2.2. Specifically, USHE institutions lack certain basic cyber hygiene controls.

USHE told us that individual institutions and their leadership are responsible for holding themselves accountable. However, this is not clearly stated in policy.

Board policy currently places responsibility on individual institutions to create plans but does not explicitly outline accountability for compliance. USHE told us that individual institutions and their leadership are responsible for holding themselves accountable. However, the policy does not clearly state this responsibility or its purpose. For example, if the policy's purpose is to drive informed decision making on risk or plan for future investments in cybersecurity, it should state that. Defining roles within an organization is a principle of effective governance. Our office published a Best Practice Handbook[14] which states:

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."

Given the variation in compliance, the board should clarify policy to ensure both USHE's role and individual institutions' roles are clearly defined. It should also

[13] Utah Office of the Legislative Auditor General. *A Performance Audit of the Cybersecurity in the State of Utah*. Report No. 2023-04, May 2023.

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

define the purpose of the policy and how the information security plans should be used. Decision making and budgeting at each institution should be done with the best information possible. The board should clarify USHE's and institutions' roles within policy to 1) improve accountability and 2) ensure information is communicated to decision-makers and risk is weighed by those in positions of authority.

RECOMMENDATION 2.1

The Utah Board of Higher Education should clarify roles, including accountability for compliance, for the Utah System of Higher Education and its member institutions in the cybersecurity policy. The policy should define the purpose of the policy and how information security plans and programs are to be used. The purpose of these changes is to ensure decisions are made according to sound information and institutions are held accountable for cybersecurity.

2.2 Additional Validation May Be Needed for Cybersecurity Controls on Future Audits

In Utah in recent years, multiple USHE institutions, school districts, counties, and a drinking water system have all suffered cyber attacks. These incidents are not isolated—they reflect a trend of escalating cybersecurity threats and rising costs in the public sector.

We believe that the risk of cyber attacks demands a more robust and independent approach to cybersecurity oversight. Independent validation is essential to ensure that cybersecurity controls are not only present but effective, resilient, and aligned with best practices. This is consistent with best practices—one of the controls under the CIS cybersecurity framework is penetration testing. The purpose of this control is to go beyond automated vulnerability scanning by actively attempting to exploit weaknesses to assess the real-world impact of potential breaches.

The purpose of the penetration testing CIS control is to go beyond automated scanning to actively test and exploit weaknesses—providing an objective and external check on security effectiveness.

To best control for cybersecurity risks and maintain security in government systems, we recommend the Legislature consider incorporating cybersecurity testing into our audits and ongoing audit work. This oversight would provide a critical layer of accountability, helping to identify weaknesses before they can be exploited. Audits of different areas of state government, local government, independent entities and other government supported programs,

not just higher education and public education, could benefit from this additional cybersecurity validation work.

RECOMMENDATION 2.2

The Legislative Audit Subcommittee should consider including cybersecurity testing and validation as part of current and future audits done by the Office of the Legislative Auditor General. This will enable a broader assessment of government agency performance and effectiveness and ensure emerging risks are addressed.

Complete List of Audit Recommendations

Complete List of Audit Recommendations

This report made the following four 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 Legislature should consider studying minimum cybersecurity standards for local education agencies. These minimum standards could follow the principles behind high-priority practices outlined by the Cybersecurity & Infrastructure Security Agency that are 1) attainable by local education agencies, regardless of size and 2) proven to reduce risk.

Recommendation 1.2

The Legislature should consider studying possible solutions to challenges faced by Utah local education agencies like insufficient prioritization of cybersecurity, staffing, training, and recruiting and retaining skilled personnel. If the Legislature studies this issue, it should consider the differences between large and small school districts in implementing cybersecurity controls.

Recommendation 2.1

The Utah Board of Higher Education should clarify roles, including accountability for compliance, for the Utah System of Higher Education and its member institutions in the cybersecurity policy. The policy should define the purpose of the policy and how information security plans and programs are to be used. The purpose of these changes is to ensure decisions are made according to sound information and institutions are held accountable for cybersecurity.

Recommendation 2.2

The Legislative Audit Subcommittee should consider including cybersecurity testing and validation as part of current and future audits done by the Office of the Legislative Auditor General. This will enable a broader assessment of government agency performance and effectiveness and ensure emerging risks are addressed.

Agency Response Plan

UTAH SYSTEM OF HIGHER EDUCATION

September 16, 2025

Kade Minchey, CIA, CFE
Legislative Auditor General
State Capitol Complex
W315 House Building
Salt Lake City, Utah 84114

Dear Legislative Auditor General Minchey,

Thank you for the opportunity to review and respond to *Audit 2025-29, A Performance Audit of Public and Higher Education Cybersecurity*. We appreciate Chris McClelland, Jesse Martinson, and Brandon Checketts for their diligent, collaborative, and professional work.

The Board and the Commissioner's Office agree with the auditors' recommendations, and will amend Board policy to clarify and improve accountability and communicate the importance of continuing to strengthen cybersecurity controls and implementing best practices to reduce cybersecurity risks within the system of higher education.

Sincerely,

Geoffrey Landward
Commissioner of Higher Education

Amanda Covington
Chair, Utah Board of Higher Education

Two Gateway
60 South 400 West
Salt Lake City, Utah 84102-1284

801.646.4784
ushe.edu

Utah Board of Higher Education Response to Audit 2025-29, A Performance Audit of Public and Higher Education Cybersecurity.

Chapter #2

Recommendation 2.1: We recommend that the Utah Board of Higher Education should clarify roles, including accountability for compliance, for the Utah System of Higher Education and its member institutions in the cybersecurity policy. The policy should define the purpose of the policy and how information security plans and programs are to be used. The purpose of these changes is to ensure decisions are made according to sound information and institutions are held accountable for cybersecurity.

Board Response:
We agree.

Description of How USHE will Implement the Recommendation:
The Commissioner's Office is in the process of reviewing Board Policy R345 to consider updates informed by this report, including clarifying the roles, responsibilities, and accountability of the Board of Higher Education and individual institutions. The Commissioner's Office will recommend updates to Board Policy R345 and present the updated policy to the Utah Board of Higher Education by March 2026.

Documentation to be used to Validate Implementation of the Recommendation:
The Commissioner's Office will share a copy of updated Board Policy 345 with the Office of the Legislative Auditor General after the updated policy is approved by the Utah Board of Higher Education.

Individuals Responsible for Implementing the Recommendation:
Stephen Hess, Chief Information Officer (CIO), USHE and the University of Utah
Alison Adams, General Counsel & Secretary of the Board, USHE

Deadline:
The Commissioner's Office will present an updated version of Board Policy R345 to the Utah Board of Higher Education by no later than March 2026.

Recommendation 2.2: We recommend the Legislative Audit Subcommittee should consider including cybersecurity testing and validation as part of current and future audits done by the Office of the Legislative Auditor General. This will enable a broader assessment of government agency performance and effectiveness and ensure emerging risks are addressed.

Board Response:
N/A

Two Gateway
60 South 400 West
Salt Lake City, Utah 84101-1284
801.321.7200
ushe.edu

THE MISSION OF THE LEGISLATIVE AUDITOR GENERAL IS TO

AUDIT · LEAD · ACHIEVE

WE HELP ORGANIZATIONS IMPROVE

olag.utah.gov