

A Performance Audit of the

Cybersecurity in the State of Utah

Office of the Legislative
Auditor General

Report to the **UTAH LEGISLATURE**





**LEGISLATIVE
AUDITOR GENERAL**

Audit Subcommittee

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

Senate Evan J. Vickers
Senate Majority Leader

Senator Luz Escamilla
Senate Minority Leader

Speaker Brad R. Wilson, Co-Chair
Speaker of the House

Representative Mike Schultz
House Majority Leader

Representative Angela Romero
House Minority Leader

Audit Staff

Kade R. Minchey, Auditor General, CIA,
CFE

Jesse Martinson, Manager, CIA

David Gibson, Audit Supervisor, CISA

Clint Yingling, 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 Brad R. Wilson, Co-Chair

Senator Luz Escamilla | Senator Evan J. Vickers

Representative Angela Romero | Representative Mike Schultz

May 16, 2023

TO: THE UTAH STATE LEGISLATURE

Transmitted herewith is our report:

“A Performance Audit of Cybersecurity in the State of Utah”[Report #2023-04].

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.

We would like to note that in our audit work that pertained to the Legislative branch, an independence in appearance concern could arise. The Auditor General serves on the staff governing council (Legislative Services Management Council) that, among other things, oversees legislative information technology. Generally accepted audit standards define independence in appearance as the “absence of circumstances that would cause a reasonable and informed third party to reasonably conclude that the integrity, objectivity, or professional skepticism of an audit organization or member of the engagement team had been compromised.” We controlled for any perceived impairments by ensuring the audit team conducted audit work of the legislative branch fully and completely without restriction. All decisions were made by the entire audit team; the rest of the team has no oversight of legislative IT. Because of these controls, no independence concern occurred.

This audit was requested by the Legislative Audit Subcommittee.

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 R. Minchey, CIA, CFE

Auditor General

kminchey@le.utah.gov





**PERFORMANCE
AUDIT**

AUDIT REQUEST

The Legislative Audit Subcommittee requested an audit of cybersecurity in the state of Utah. We were asked to audit the three branches of government as well as all interlocal entities.

BACKGROUND

Cyberattacks have cost the state of Utah millions of dollars and will continue to cost the state if cybersecurity measures are not taken. Entities should be taking proactive steps to identify weaknesses and gaps in their security and use a cybersecurity framework as a guiding policy to address cybersecurity vulnerabilities. Various entities throughout the state were found to be at risk to cybersecurity attacks and need to strengthen their security framework.

CYBERSECURITY IN THE STATE OF UTAH



KEY FINDINGS

- ✓ Many entities lack a cybersecurity framework
- ✓ IT personnel can improve communication skills to accurately present their ideas to management
- ✓ Many entities do not require annual cybersecurity awareness training
- ✓ Legislative information technology office are not compliant with recognizable and accepted cybersecurity standard.
- ✓ The judicial branch does not a cybersecurity strategic plan
- ✓ The Division of Technology Services work with agencies to ensure employees are completing the annual cybersecurity training



KEY RECOMMENDATIONS

- ✓ Information technology officers follow a structured process using competent IT standards when communicating cybersecurity compliance and threats to management.
- ✓ The Legislature consider creating in statute requiring all state employees complete annual cybersecurity assessment training.
- ✓ Judicial branch update and maintain a cybersecurity strategic plan.
- ✓ Division of Technology Services work with agencies in the executive branch to ensure that all employees complete the annual cybersecurity awareness training

Summary continues on back >>



REPORT SUMMARY

1.1 Cybersecurity in the State Needs to Improve

The implementation of cybersecurity related controls vary across the state but overall, most entities still have room for improvement. One of the central themes which we will discuss later in the report is the breakdown of communication about the associated risks of cybersecurity between IT staff and administration.

1.2 Entities can Improve their Adoption of Cybersecurity Best Practices

Implementing best practices can strongly reduce cybersecurity risk and decrease entities' vulnerability to cyberattacks. The Washington State Auditor released a report in 2022 and found that entities that adopt a cybersecurity framework tended to have less severe vulnerabilities.

2.1 Legislative Information Technology Office Needs to Develop a Cybersecurity Plan

Currently, Legislative Information Services (LegIT) does not have a cybersecurity strategic plan. LegIT needs to create a cybersecurity strategic plan to plan out the necessary security that will enable the Legislative branch to continue their work in a secure and safe environment.

2.3 The Executive Branch Should Better Prioritize Employee Training

The executive branch can improve its cybersecurity training. We found that some agencies have low compliance for cybersecurity training.

CIS Scores Statewide

We surveyed many entities in the state from branches of state government to local government to public schools. We found that most of the entities that we visited scored in the mediocre category for the CIS controls.

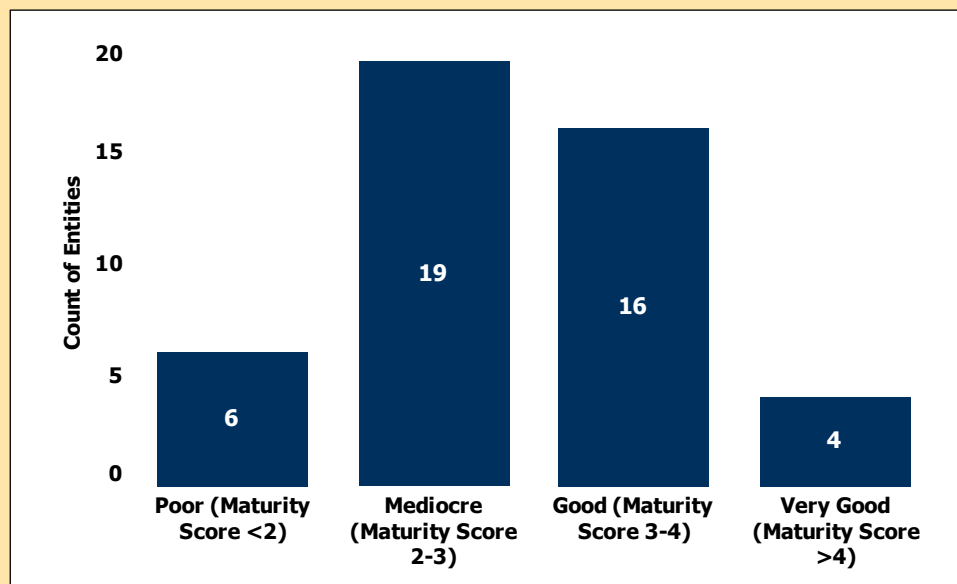


Table of Contents

Chapter 1

Opportunities Exist for Government Entities to Improve Cybersecurity Readiness.....	3
1.1 Cybersecurity Needs to Be Improved Across the State	3
1.2 Entities Can Improve Their Adoption of Cybersecurity Best Practices	4
1.3 Our Survey Revealed That Governmental Entities across the State Need Improvement in Key Areas	10

Chapter 2

Review of the Three Branches of Government Shows Cybersecurity Improvements Are Needed.....	17
2.2 The Judicial Branch Should Update Its Strategic Plan and Increase Cybersecurity Training to Strengthen Its Cybersecurity Preparedness.....	21
2.3 The Executive Branch Has Adopted Policies and Standards for Cybersecurity	23
Complete List of Audit Recommendations	27
Complete List of Audit Recommendations	29
Agency Response	31



**BACKGROUND**

Cyberattacks have cost the state of Utah millions of dollars and will continue to do so if cybersecurity measures are not taken. Entities should take proactive steps to identify weaknesses and gaps in their security and use a cybersecurity framework as a guiding policy to address cybersecurity vulnerabilities. Losses are not necessarily financial; they could include credibility, information, and time unable to fulfill necessary functions. In 2022, the Legislature created the Cybersecurity Commission with the goal of developing a public–private partnership to improve cybersecurity in the state. During the 2023 Legislative Session, the Legislature passed Senate Bill 127, which creates a reporting requirement for entities that experience a cyberattack.

FINDING 1.2

Many state entities have not adopted cyber security best practices such as cyber security framework, necessary communication of risks to management, and cyber security training for all employees.

RECOMMENDATION 1.1

Entities that lack a cybersecurity framework need to immediately adopt a framework, such as the Center for Internet Security (CIS) standards.

RECOMMENDATION 1.2

Information technology officers need to follow a structured process using competent IT standards when communicating cybersecurity compliance and threats to management.

RECOMMENDATION 1.3

The Legislature consider creating a statute requiring all state employees to complete annual cybersecurity awareness training.

FINDING 1.3

Many entities need to improve their cybersecurity compliance with the CIS controls.

RECOMMENDATION 1.4

Governmental entities that are not satisfactorily compliant with competent cybersecurity standards should prioritize compliance.

FINDING 1.4

Many entities lack an incident response plan.

RECOMMENDATION 1.5

Entities need to create and maintain an incident response plan.

**CONCLUSION**

Many entities can decrease the likelihood of serious cyberattacks through a few simple and effective methods. These include adopting a cybersecurity framework, improving communication between IT leadership and administrative leadership, and requiring employees to complete annual cybersecurity training. Despite entities' best efforts to prevent cyberattacks, they can still occur. Therefore, several entities need to adopt an incident response plan to minimize the cost of a potential successful attack.





Chapter 1

Opportunities Exist for Government Entities to Improve Cybersecurity Readiness

1.1 Cybersecurity Needs to Be Improved Across the State

We believe government entities should be taking proactive steps to identify weaknesses and gaps in their security and use a cybersecurity framework as a guiding document to address those issues. The implementation of cybersecurity-related controls varies across the state; overall, many entities still have room for improvement. During the 2022 session, the Legislature created the Cybersecurity Commission within the Department of Public Safety to coalesce efforts around improving cybersecurity in the state. The commission began meeting in August 2022 and presented its first report to the Legislature in November 2022. One of the commission's recommendations, Senate Bill 127, was passed during the 2023 session, creating a reporting mechanism for entities that experience a cybersecurity breach. We are encouraged by the commission's efforts and believe the commission can be a vehicle to help implement the recommendations of this audit report.



The Cybersecurity Commission was created by the Legislature during the 2022 session.

One of the central themes of this report is the breakdown of communication between IT staff and administration about the associated risks of cybersecurity. Entities we interviewed that had experienced a cyberattack reportedly paid anywhere from hundreds of thousands of dollars upward to over a million dollars as a result of the attack. One of the positive things to come from those cyberattacks was that entities in surrounding areas motivated their administration to review their infrastructure and spurred changes internally.

To better understand the state's current cybersecurity posture, we sent surveys to 620 entities in counties, cities and towns, higher education, applied technical colleges (ATCs),¹ school districts, and local districts. We also reviewed the legislative, judicial, and executive branches' cybersecurity areas, which are discussed in detail in Chapter 2.

¹ We sent the survey only to the technical colleges. We did not send a survey to colleges and universities.



We identified five important elements of cybersecurity.

- 1. Surveyed cybersecurity safeguards of entities against the CIS Controls.*
- 2. Surveyed to determine how many entities adopted a cybersecurity framework.*
- 3. Surveyed to determine how many entities did internal vulnerability scans.*
- 4. Surveyed to determine how many entities require cybersecurity training.*
- 5. Determine how many entities created an incident response plan.*

Unfortunately, the response rate to our survey was only 37 percent. This low response rate does not allow us to adequately determine the overall risk to the state. We are concerned that the response rate was low potentially due to the lack of secure cybersecurity networks.

1.2 Entities Can Improve Their Adoption of Cybersecurity Best Practices

Implementing best practices can strongly reduce cybersecurity risks and decrease entities' vulnerability to cyberattacks. The Washington state auditor released a report in 2023 and found that entities that adopted a cybersecurity framework tended to have less severe vulnerabilities. From our survey, we found multiple entities that have not adopted a cybersecurity framework.

Entities can more accurately understand their risk profile by comparing their cybersecurity safeguards and risk policies against a recognized cybersecurity framework. The Center for Internet Security (CIS) is a recognized resource and is utilized by IT professionals throughout the state. The controls are prioritized actions for cybersecurity that form a defense-in-depth set of specific and actionable best practices to mitigate cyberattacks. Another resource is the federal government's National Institute of Standards and Technology (NIST) standards. Our concern is that some entities are following no standard at all. The Legislature has referenced the CIS Control Standards (CIS Controls) in statute² as an acceptable framework for entities to utilize; therefore, this is the framework used for our security assessments. Recently, the Utah System of Higher Education passed a board rule requiring that all higher education entities



We found that many entities have not adopted a cybersecurity framework.

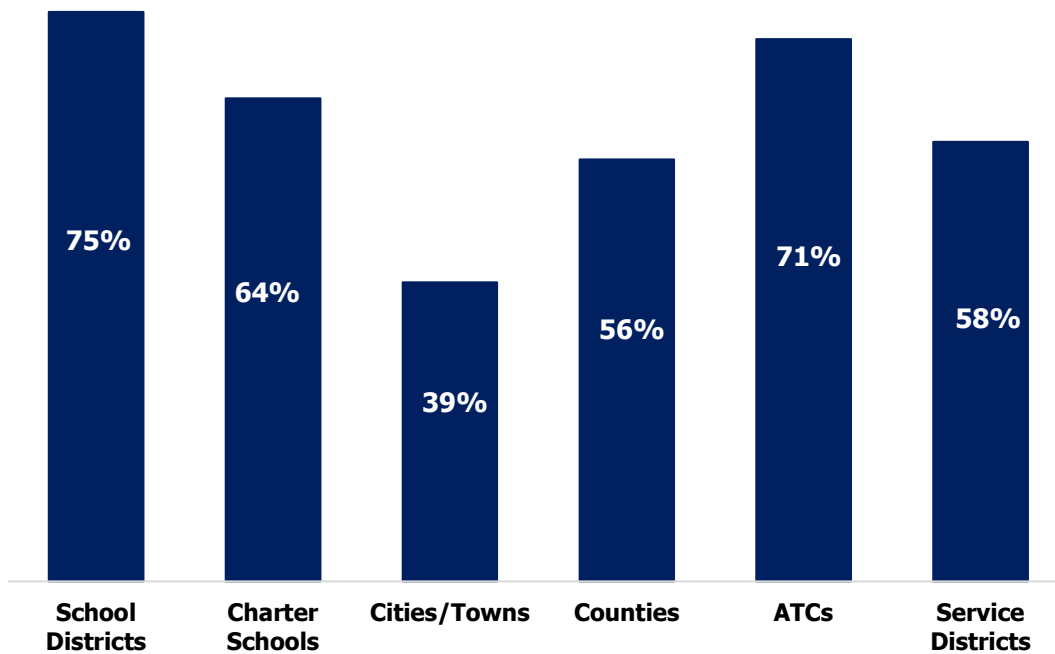
² *Utah Code* 78B-4-703(D).



become compliant with the CIS standards. The Utah State Board of Education passed a rule a few years ago requiring local education agencies to implement a cybersecurity framework.

In total, we received 223 responses to our survey. Among all respondents, 57 percent stated that they have adopted a cybersecurity framework. Figure 1.1 shows the percentage of specific entities that have adopted³ a cybersecurity framework.

Figure 1.1 Percentage of Entities That Have Adopted a Cybersecurity Framework.⁴
The adoption rate of a cybersecurity framework varies across the state.



Source: Auditor generated

With a response rate of only 37 percent, we are concerned that we were unable to determine the totality of cybersecurity risk to the state. Therefore, we can speak only to the entities that responded to the survey. Still, we are concerned about the entities that did not respond to our survey. They may not have adopted a cybersecurity framework and may not have implemented proper controls to decrease cybersecurity attacks.

The CIS Controls cover various critical components to IT security, including *Inventory and Control of Software Assets, Data Protection, Malware Defenses,*

³ Entities may have adopted a cybersecurity framework without fully complying with the framework. The scope of our audit work did not include a review of each entity’s compliance with the cybersecurity framework.

⁴ State-level entities’ compliance with the framework is discussed in Chapter 2.



*Data Recovery, and Security Awareness and Skills Training.*⁵ Cybersecurity frameworks allow IT staff to compare their current safeguards and risk policies against a set of industry-leading best practices to understand areas of weakness.

RECOMMENDATION 1.1

Entities lacking a cybersecurity framework need to immediately adopt a framework, such as the Center for Internet Security (CIS) standards.

Cybersecurity Communication Techniques Can Improve

Across the state, we found that communication between cybersecurity experts and management is often in need of improvement. It appears that the communication disparity between cyber experts and management is often due to barriers such as communication style and technical understanding. By using a framework, IT staff can formulate a roadmap based on areas that could improve and present the risks and possible safeguards to those who oversee their operation and together determine the best path forward.

For example, in one entity we observed, it appeared that management and its IT group were having difficulty communicating. Management was looking for tangible assurance that its systems and processes were secure. IT believed it was providing that assurance by communicating, often in technical jargon, verbally to management. Management indicated to us that they still are not clear about the status of security in their organization. To resolve miscommunication between IT and management, we recommend that competent IT standards be used as a framework to communicate an organization's cybersecurity status. The following steps could be used.



We found a communication disparity between IT personnel and management.

⁵ The CIS Cybersecurity Framework version 8.0 includes eighteen controls that are further categorized into a total of 153 safeguards.



Steps to Improve Communication between IT Personnel and Management

1. *The IT group should create an assessment document that lists all standards in an accessible format for review by management.*
2. *Management should then require IT or an independent outside entity to conduct an assessment to determine whether the level of compliance meets standards.*
3. *A plan of action would be created that specifies timeframes for each standard to be completed, who in the organization is responsible for ensuring compliance, and a budget if additional resources are needed.*
4. *The plan would then be reviewed, revised if needed, and approved by management.*
5. *Regular follow-up is needed to ensure the organization is on track to be in compliance with the standards.*

RECOMMENDATION 1.2

Information technology officers need to follow a structured process using competent IT standards when communicating cybersecurity compliance and threats to management.

Many Entities Are Not Conducting Vulnerability Scans of Their Systems

Internal vulnerability scans help entities identify vulnerabilities and improve network security. The potential impact of not conducting vulnerability scanning can be severe, because cyber criminals may gain unauthorized access and steal sensitive data or cause damage to critical systems. Vulnerability scanning is an essential part of ensuring that systems are secure, and many entities do not appear to be doing it. Not all entities have the same risk level; however, entities that store sensitive records such as financial data, personal health information, or other personally identifiable information are at higher risk.

CIS Control #7 covers *Continuous Vulnerability Management*, which recommends that entities have a documented process and perform scans on a quarterly basis, or more frequently, if possible. We found fairly similar results when asking entities if they conduct vulnerability scans of

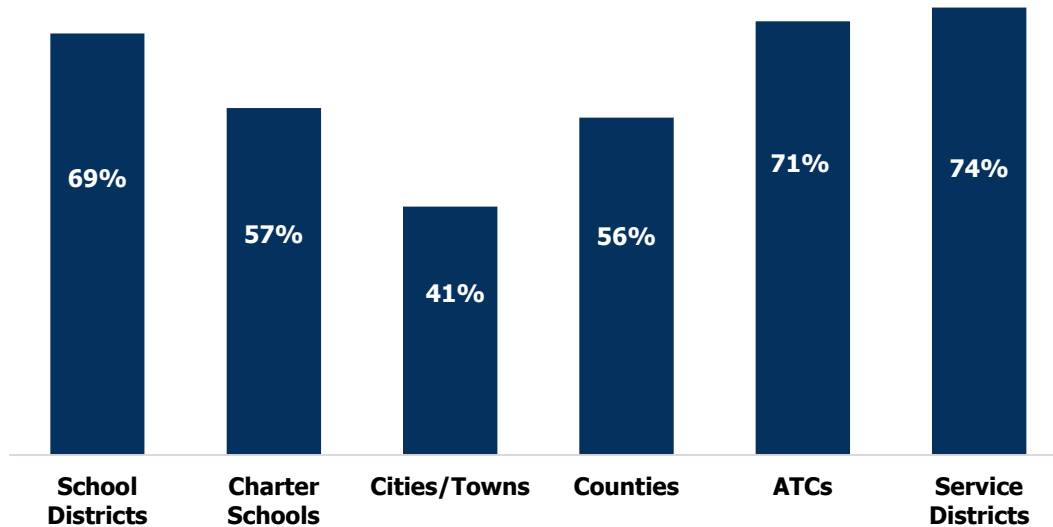


We found that many entities are not performing internal scans of their computer systems.



their network. Figure 1.2 shows the percentage of entities that have done vulnerability scanning on their systems.

Figure 1.2 Vulnerability Scanning.⁶ Cities were one of the entity types that experienced the most successful system security breaches while also having the lowest adoption of vulnerability scanning.



Source: Auditor generated

These survey results are only for the entities that responded. For medium-to large-size entities with more sensitive data, the CIS Controls recommend doing vulnerability scans at least quarterly to understand where attackers may gain unauthorized access to an organization’s system.

End Users Are a Substantial Vulnerability in Cybersecurity, Yet Many Entities Are Not Providing Adequate Training

The results from our survey indicate that requiring cybersecurity awareness training is not a priority for most entities. Cyberattacks are constantly evolving, and attackers are becoming more sophisticated in their methods. Employees can be frequently targeted with phishing attacks. If an employee is a victim of a phishing attack, it could be detrimental to the security of an entire entity. Studies have shown that anywhere from 20 to 95 percent of all cybersecurity breaches are a result of human error. In Utah, social engineering attacks, such as phishing, resulted in a loss of just under \$6 million across the state from 2016 to 2022. Some people we interviewed view cybersecurity as the responsibility of IT staff only; however, every employee plays a critical role in securing the organization from threats. Many of the entities we spoke with that



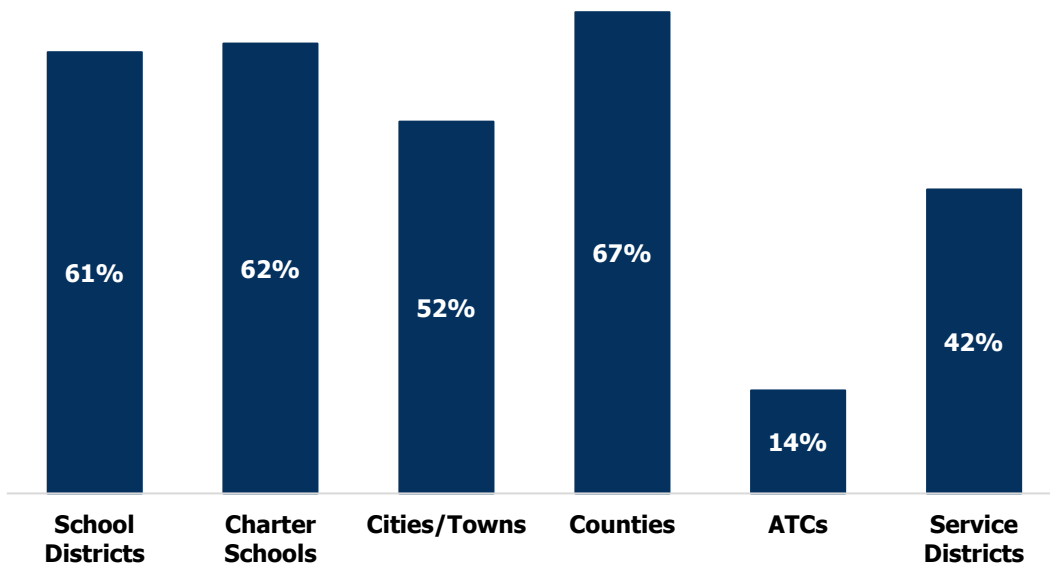
Studies have shown, that anywhere from 20 to 95 percent of all breaches are a result of human error.

⁶ State-level entities’ compliance with the framework is discussed in Chapter 2.



had experienced a cyberattack indicated that the attack was the result of human error. Of the 223 respondents in our survey, 56 percent reported requiring annual cybersecurity awareness. Figure 1.3 shows the percentage of entities that require annual cybersecurity training.

Figure 1.3 Percentage of Entities That Require Annual Cybersecurity Awareness Training.⁷ The adoption rate of a cybersecurity framework varies across the state.



Source: Auditor generated

Entities should develop a cybersecurity awareness training program, recognize social engineering attacks, and implement best practices for authentication and data handling. We believe entities should formalize these best practices in policy and require all staff to be trained during their onboarding and on an annual basis thereafter.



Many entities do not require their employees to take annual cybersecurity awareness training.

One entity told us that their administration would not let them conduct annual cybersecurity awareness training for their employees. We found that eighteen different states have statute or executive orders requiring annual cybersecurity awareness training for state employees.

RECOMMENDATION 1.3

The Legislature consider creating a statute requiring all state employees to complete annual cybersecurity awareness training.

⁷ State-level entities' compliance with the framework is discussed in Chapter 2.



1.3 Our Survey Revealed That Governmental Entities across the State Need Improvement in Key Areas

Using the CIS Controls, we found that cybersecurity risks exist in various entities throughout the state. We used the CIS maturity scores to measure the cybersecurity risks of entities. We visited multiple entities and had them complete the CIS maturity exercise. From this exercise, we found cybersecurity vulnerabilities in entities across the state.



The CIS maturity scores are used to measure cybersecurity risks of entities.

We found that several entities had concerning CIS maturity scores for the following CIS Controls:

- Data protection
- Cybersecurity awareness training
- Vendor management

We used the CIS Controls to assess the entities' cybersecurity risks. Our survey showed a cross section of entities, from education to political subdivisions, that scored low on the CIS Controls. As seen in Figure 1.4, each safeguard has a CIS maturity score ranging from one to five. We asked the entities to select a score for each safeguard to determine how compliant they are to the standards. The CIS Controls have eighteen controls with six different asset classes: Enterprise, Devices, Applications, Data, Network, and Users.

Figure 1.4 CIS Maturity Scores. We used the CIS maturity scores to determine how compliant entities are with the CIS Controls.

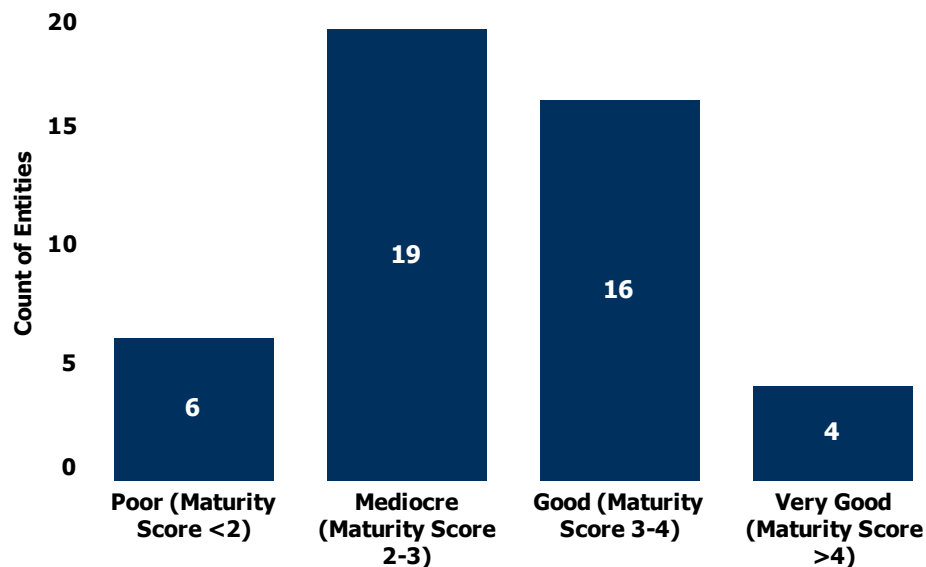
Maturity Score	Definition
1	Safeguard is not implemented or is inconsistently implemented.
2	Safeguard is implemented fully on some assets or partially on all assets.
3	Safeguard is implemented on all assets.
4	Safeguard is tested and inconsistencies are corrected.
5	Safeguard has mechanisms that ensure consistent implementation over time.

Source: Center for Information Security

The CIS Controls have fifty-six safeguards for small organizations, 130 safeguards for medium-sized organizations, and 153 safeguards for large organizations. Figure 1.5 shows the CIS maturity scores statewide.



Figure 1.5 CIS Maturity Scores Statewide.⁸ The CIS maturity scores of many of the entities we surveyed are categorized as either “mediocre” or “good.” Entities’ scores demonstrate the varying degrees of implementation of safeguards on enterprise assets.



Source: Auditor generated

As Figure 1.5 shows, many entities that responded to the survey need to improve their cybersecurity safeguards.

RECOMMENDATION 1.4

Compliance needs to be made a high priority for any governmental entity that is not satisfactorily compliant with competent cybersecurity standards.

1.4 Entities Need to Create an Incident Response Plan in Case of a Cyberattack

Many entities we surveyed do not have an incident response plan. A sufficient incident response plan offers a course of action for significant incidents. Entities need to prepare for a possible successful attack on their network. An incident response plan can include the following elements:

⁸ State-level entities’ compliance with the framework is discussed in Chapter 2.



- The organization’s approach to incident response
- Activities required in each phase of incident response
- Roles and responsibilities for completing incident response activities
- Communication pathways between the incident response team and the rest of the organization
- Metrics to capture the effectiveness of the organization’s incident response capabilities

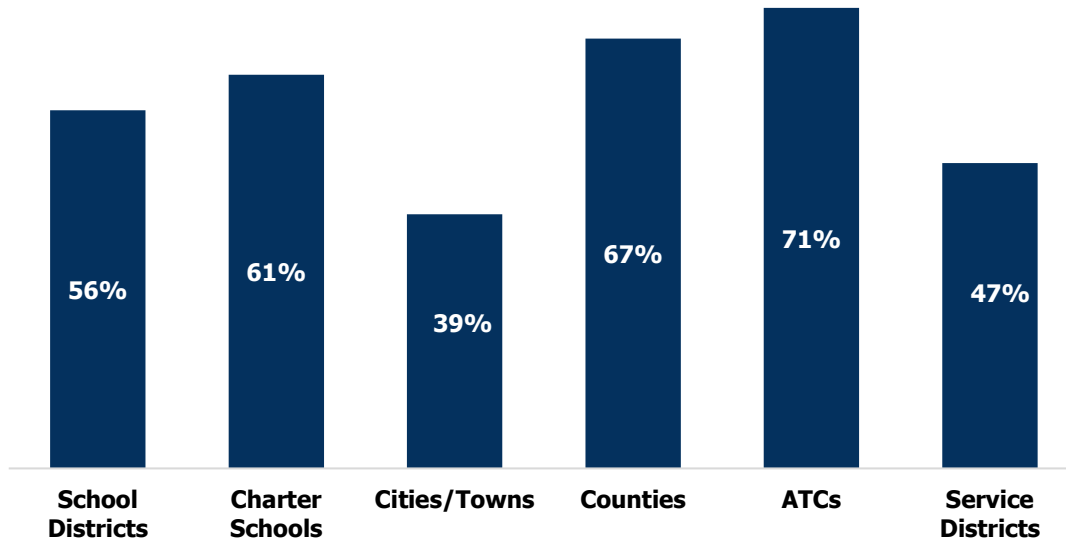


We found that many entities do not have an incident response plan.

An incident response plan may be designed to align with an entity’s priorities and its level of acceptable risk. Figure 1.6 shows the percentage of entities that currently have an incident response plan.



Figure 1.6 Percentage of Entities That Have an Incident Response Plan.⁹ The percentage of entities that have an incident response plan varies across the state.



Source: Auditor generated

Creating and developing a response plan is one way to ensure an entity is prepared and can recover from a cyberattack. As indicated in Figure 1.6, a significant percentage of entities across the state do not have an incident response plan. This could result in millions of dollars of damage that could be avoided if a plan were in place.

RECOMMENDATION 1.5

Entities need to create and maintain an incident response plan.

⁹ State-level entities' compliance with the framework is discussed in Chapter 2.



**BACKGROUND**

Utah's three branches of government are at risk for cyberattacks. This audit does not provide assurance of cybersecurity infrastructure. Instead, it was designed to help organizations understand cybersecurity risks and to provide recommendations for risk mitigation. This chapter addresses state-level agencies and provides recommendations to mitigate cybersecurity risks through better planning and policies.

FINDING 2.1

Legislative Information Technology office is not compliant with cybersecurity standards. We found they lack a cybersecurity strategic plan, insufficient cybersecurity policy, and does not have an incident response plan to guide cybersecurity of the Legislative Branch.

RECOMMENDATION 2.1

The Legislative Information Technology office needs to create and maintain a cybersecurity strategic plan.

RECOMMENDATION 2.2

The Legislative Information Technology office needs to create a detailed incident response plan.

RECOMMENDATION 2.3

The Legislative Information Technology office needs to create and maintain a more detailed cybersecurity policy.

RECOMMENDATION 2.4

The Legislative Information Technology office needs to become compliant with a recognizable and accepted cybersecurity standard.

FINDING 2.2

The Judicial Branch lacks an updated cybersecurity strategic plan and insufficient cybersecurity training.

RECOMMENDATION 2.5

The judicial branch needs to update and maintain their cybersecurity strategic plan.

RECOMMENDATION 2.6

The judicial branch needs to ensure its employees complete the annual cybersecurity awareness training.

FINDING 2.3

Division of Technology Services needs to ensure all state employees complete cybersecurity training.

RECOMMENDATION 2.7

The Division of Technology Services needs to work with agencies in the executive branch to ensure that all employees complete the annual cybersecurity awareness training.

**CONCLUSION**

Opportunities exist for Utah's three branches of government to improve their protection against cyberattacks by ensuring employees are getting trained. The legislative branch's cybersecurity team is relatively new, as the Legislature used to contract with the executive branch for cyber control. Accordingly, the Legislature should ensure that it has detailed policies and planning in place to strengthen controls and expectations.





Chapter 2

Review of the Three Branches of Government Shows Cybersecurity Improvements Are Needed

2.1 Legislative Information Technology Office Needs to Develop a Cybersecurity Strategic Plan, Strengthen Its Cybersecurity Policy, and Create an Incident Response Plan

The Legislative Information Technology office (LegIT) needs to create a cybersecurity strategic plan to map out the necessary security that will enable the legislative branch to continue its work in a secure and safe environment. Having a cybersecurity strategic plan will reduce risk and build resilience to cyber and physical threats to LegIT's infrastructure. LegIT recently wrote a cybersecurity policy, but it lacks the necessary elements to be effective. Other organizations' policies are much more sophisticated. LegIT also needs to create and maintain an incident response plan. Incident response plans are important because they outline how to minimize the duration and damage of cybersecurity incidents. We also found that LegIT needs to improve its compliance with standards from the Center for Internet Security's Controls (CIS Controls). As discussed in Chapter 1, the CIS Controls are referenced in state statute and thus are the controls we used as a reference for this audit. There are also standards of the National Institute of Standards and Technology (NIST), which are written by the federal government and housed within the US Department of Commerce. The CIS Controls largely adopt the NIST standards. Our recommendation is that every government organization adopt one of the competent and recognized cybersecurity standards.

Legislative Information Technology Office Needs to Create a Comprehensive Cybersecurity Strategic Plan

Currently, LegIT lacks a cybersecurity strategic plan. We found that the Division of Technology Services (DTS) has a cybersecurity strategic plan, as does Montana's Legislative Services Division. We also found that the executive branches in certain states have cybersecurity strategic plans, including Washington, Oregon, and Nevada. As an example of what a cybersecurity strategic plan might include, Oregon's plan contains details on the following goals the state hopes to achieve:



The Legislative Information Technology office lacks a cybersecurity strategic plan.



- Mature statewide IT security
- Establish legacy system modernization
- Security planning
- Security program management
- Risk assessment
- Security assessment and authorization

A cybersecurity strategic plan will help guide LegIT to provide valuable, secure, responsive, and innovative information technology for the Legislative branch. The purpose of a cybersecurity strategic plan is to help the organization protect against breaches, loss of reputation, and the ability to recover from a cyberattack. A cybersecurity strategic plan is a document that outlines an organization's vision, mission, goals, and objectives for managing cyber threats. It is a long-term plan that provides guidance and direction for an organization's decision-making and resource allocation over a period of several years. A cybersecurity strategic plan should include an analysis of the organization's strengths and weaknesses and should specifically include an assessment of external threats. In other words, the plan should specify unique aspects of the organization that may elevate the cyber threat. Based on this analysis, the plan should establish specific measurable goals to manage cyber risk. We found that Utah's executive branch has a cybersecurity strategic plan. The judicial branch also has a plan, although it was last updated in 2014.

LegIT needs to create a cybersecurity strategic plan that encompasses all aspects of the legislative branch. LegIT should work with the Senate, House of Representatives, and each staff office to understand their unique needs and then devise a plan that addresses each of those needs. In addition, the plan should keep security as a high priority. Having a cybersecurity strategic plan will help each office succeed in its goals and missions.

The Legislative Information Technology Office Needs to Create a Comprehensive Cybersecurity Policy

LegIT needs to have a comprehensive cybersecurity policy. Currently, LegIT has a one-page policy with minimal detail. Our review showed that other organizations' policies were much more detailed and sophisticated. For example, DTS and the judicial branch each have a cybersecurity policy. DTS's policy, which covers the executive branch, follows the NIST standards. The executive branch policy is very detailed contains elements such as:

- Security planning
- Security program management
- Risk assessment
- Security assessment and authorization



The judicial branch also has a comprehensive policy that addresses compliance with all applicable laws and how users can be protected from data breaches. The primary purpose of a cybersecurity policy is to enforce security standards and procedures to protect computer systems, prevent security breaches, and safeguard private networks. Other purposes of cybersecurity policy can include the following:

- Protect data and IT infrastructure.
- Define rules for using an entity's devices and personal devices at work.
- Inform employees of disciplinary actions for policy violation.

The policy can also offer countermeasures to limit damage in the event of any security incident. Having a comprehensive cybersecurity policy will provide a better defense against a possible cyberattack.

Creating an Incident Response Plan Will Help the Legislative Information Technology Office Mitigate Exposure from Cybersecurity Attacks

LegIT needs to create an incident response plan. Not having an incident response plan could lead to systems being down for a prolonged period while LegIT works to formulate a response to a cyberattack. Having a detailed plan that is already well-conceived and written down will allow LegIT to act quickly, deliberately, and strategically in the event of a security incident.

We found that both DTS and the judicial branch have an incident response plan. An incident response plan contains a detailed plan of action for handling potential security incidents. Several governmental entities have experienced ransomware incidents, and because they did not have an incident response plan, it took them longer to recover from the attack. This situation can lead to the loss of employee productivity and the loss of reputation. Incident response plans contain specific directions for responding to specific attack scenarios, avoiding further damages, reducing time, and mitigating cybersecurity risk. Having an incident response plan will enable LegIT to minimize the time needed to respond to a potential cyberattack. An incident response plan is a set of actions for all significant events. Some incidents can lead to massive network or data breaches that could impact an organization for days or even months. Not having an incident response plan may result in a complete loss of data and systems. There are at least eight essential elements for an incident response plan.

- A mission statement
- Formal documentation of roles and responsibilities
- Cyberthreat preparation documentation
- Incident detection documentation



Legislative information technology lacks an incident response plan.



- An incident response threshold determination
- Management and containment process
- Fast, effective recovery plans
- Post-incident review

These are just some of the items that could be included in an incident response plan. We found that LegIT needs to adopt competent cybersecurity standards like the CIS Controls. The primary purpose of cybersecurity controls is to minimize the risk of cyberattacks. The controls are to protect sensitive information and valuable data from being compromised. They are designed to help entities rapidly define starting points for their defenses and direct scarce resources toward actions that have immediate, high-value payoff. The controls allow entities to focus their attention and resources on additional risk issues that are unique to their business or mission. Despite some of these issues that LegIT needs to resolve, the office has been proficient with cybersecurity training, with legislative staff completing close to 100 percent of the cybersecurity training in 2022.



Despite needing to adopt policies, LegIT excels in training legislative employees, with staff completing close to 100 percent of cybersecurity training in 2022.

RECOMMENDATION 2.1

The Legislative Information Technology office create and maintain a cybersecurity strategic plan.

RECOMMENDATION 2.2

The Legislative Information Technology office create a detailed incident response plan.

RECOMMENDATION 2.3

The Legislative Information Technology office create and maintain a more detailed cybersecurity policy.

RECOMMENDATION 2.4

The Legislative Information Technology office become compliant with a recognizable and accepted cybersecurity standard.



2.2 The Judicial Branch Should Update Its Strategic Plan and Increase Cybersecurity Training to Strengthen Its Cybersecurity Preparedness

The judicial branch's latest cybersecurity plan was created in 2014 and needs to be updated. A cybersecurity strategic plan may help the judicial branch reduce the number of security gaps, extend visibility into security threats, and help meet compliance requirements. For example, we found that strategic plans in three states have these goals and directives and also include shared services, security and privacy, best practices, and methodologies. The purpose of a cybersecurity strategic plan is to protect against breaches and loss of reputation, and to enhance the ability to recover from a cyberattack.

Our assessment of the Administration of the Courts IT (AOC-IT) found that this entity performed better than other similarly sized organizations did, but there are still critical areas for improvement. The CIS Controls analyzes both the implementation of safeguards and the entity's security policies. Five of the six security-related policies that AOC-IT shared with us have been in draft form since 2018-19, following the most recent security assessment. It is important for AOC-IT to finalize those policies to provide clarity to the organization regarding current policies and standards.



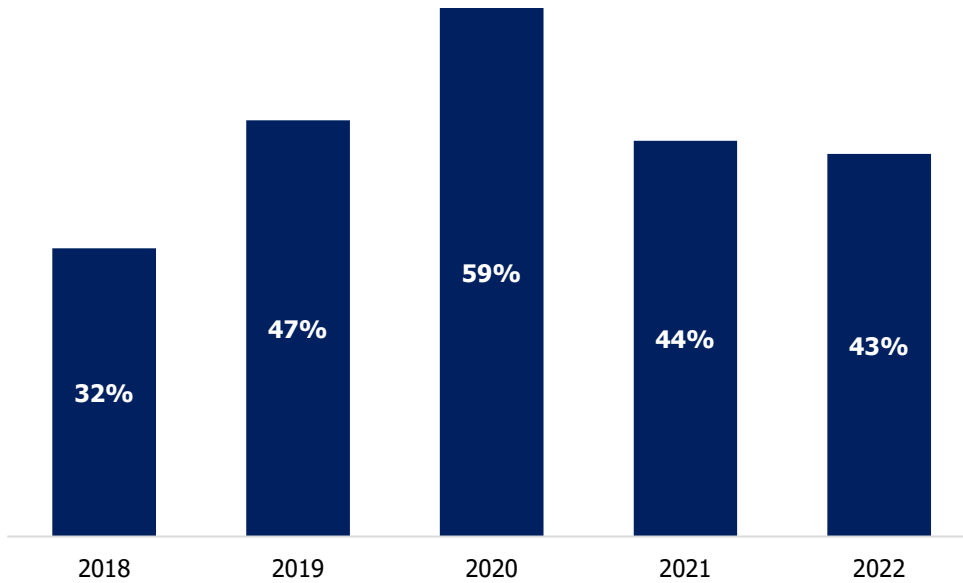
The judicial branch needs to ensure that its employees comply with the cybersecurity policy.

We found that the judicial branch can also improve compliance with its policy of requiring annual cybersecurity awareness training. The Joint Technology Committee ¹⁰notes that continuous security awareness training is foundational in helping staff understand cybersecurity best practices and evolving threats. However, over the last five years, completion rates of judicial staff have been low. As shown in Figure 2.1, the judicial branch's highest completion rate was in 2020, at 59 percent. In the other four recent years, the judicial branch has had fewer than 50 percent of its staff complete cybersecurity training.

¹⁰ The report was created by Conference of State Court Administrators, the National Association for Court Management and the National Center for State Courts.



Figure 2.1 Completion Rates for the Judicial Branch’s Cybersecurity Awareness Training, 2018 to 2022. The Judicial branch needs to ensure that all employees complete the cybersecurity training.



Source: Division of Technology Services

The judicial branch needs to ensure that its employees are completing their annual cybersecurity awareness training. As mentioned in Chapter 1, human error is a major contributor to cybersecurity breaches. As noted, in Chapter 1, studies have found that while human error is common across all sectors, human error in cybersecurity is so overwhelming that it accounts for nineteen out of twenty cyber breaches.



Nineteen out of twenty breaches are a result of human error.

RECOMMENDATION 2.5

The judicial branch needs to update and maintain their cybersecurity strategic plan.

RECOMMENDATION 2.6

The judicial branch needs to ensure its employees complete the annual cybersecurity awareness training.



2.3 The Executive Branch Has Adopted Policies and Standards for Cybersecurity

The scope of this audit was to determine areas of risk in government entities' preparedness for cybersecurity attacks. Accordingly, we reviewed the entities' planning and policies. We also conducted limited tests of systems. We did not test compliance with policies through infrastructure review, nor did we conduct simulated attacks. Accordingly, we cannot fully attest to the state of readiness. Nevertheless, an organization's adoption of cybersecurity standards, along with pertinent policies, planning, and training, represents a significant step toward thwarting cyberattacks. The executive branch has implemented policies and planning, although some organizations within the executive branch can improve their training.

We had DTS, which is in charge of the executive branch's cyber policies, provide us with documentation of its compliance with the CIS Controls. DTS is 99 percent compliant with the CIS Controls. We also found that DTS scans its systems daily for malicious intent. Three other states use DTS as criteria for their cybersecurity needs. DTS needs to continue to be vigilant to ensure a cyberattack does not happen in the future.

Executive Branch Should Better Prioritize Employee Training

The executive branch can improve its employee cybersecurity training. We found that some agencies have low compliance in cybersecurity training. As previously stated, human error is by far the most common cause of cyber breaches and overcomes even the best policies and infrastructure. We recommend that the executive branch prioritize employee cyber training and ensure that all employees receive the training.

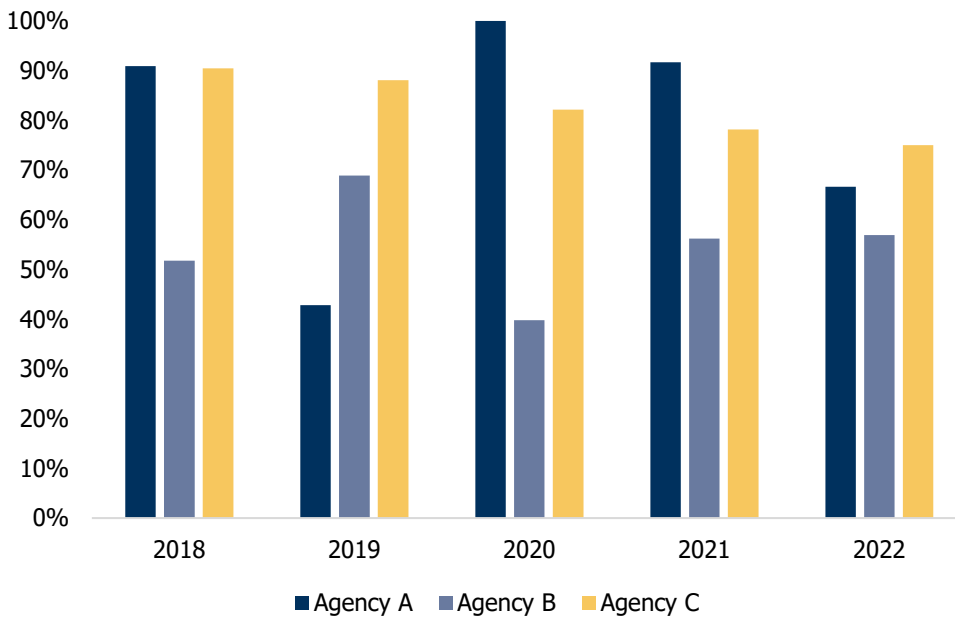


Human error can overcome even the best policies and infrastructure. The executive branch should ensure that all employees are trained.

DTS is in charge of delivering the annual cybersecurity training to all agencies in the executive branch. DTS's information policy, titled "2.4.6 Security Awareness and Training," states that all employees are required to undergo annual cybersecurity training. Figure 2.2 shows that some agencies need improvement.



Figure 2.2 Completion Rates of Three Agencies' Cybersecurity Awareness Training, 2018 to 2022. A significant percentage of employees in these three agencies of the executive branch did not complete the cybersecurity training each year.



Source: Division of Technology Services

DTS notes that it consistently deals with employees who interact with malicious emails or emails trying to phish information from them. DTS needs to work with the agencies of the executive branch to ensure that all employees complete the annual cybersecurity awareness training.

RECOMMENDATION 2.7

The Division of Technology Services needs to work with agencies in the executive branch to ensure that all employees complete the annual cybersecurity awareness training.

Recent Legislation Directs DTS to Oversee Collection of Information about Cyberattacks on Government Entities

With the passage of Senate Bill 127, DTS will now oversee the collection of information about cyberattacks on other government entities and will provide entities with assistance to recover from the attacks. The bill instructs DTS to do many things concerning cybersecurity in the state. The following are just some of the items required in the bill:



- Develop incident response plans to coordinate federal, state, local, and private sector activities.
- Coordinate, develop, and share best practices for cybersecurity.
- Develop a sharing platform to provide resources based on information, recommendations, and best practices.
- Partner with institutions of higher education and other public and private organizations to increase the state's cyber resilience.
- By June 30, 2024, develop a statewide strategic cybersecurity plan for executive branch agencies and other governmental agencies.
- Serve as the state cybersecurity incident response hotline to receive reports of breaches of system security.

By having DTS receive reports of breaches from various government entities, it will be able to provide a comprehensive picture of breaches that are occurring throughout the state.





Complete List of Audit Recommendations



Complete List of Audit Recommendations

This report made the following 11 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

We recommend that entities lack a cybersecurity framework immediately adopt a framework, such as the Center for Internet Security (CIS) standards.

Recommendation 1.2

We recommend that information technology officers follow a structured process using competent IT standards when communicating cybersecurity compliance and threats to management.

Recommendation 1.3

We recommend that the Legislature consider creating a statute requiring all state employees to complete annual cybersecurity awareness training.

Recommendation 1.4

We recommend that compliance be made a high priority for any governmental entity that is not satisfactorily compliant with competent cybersecurity standards.

Recommendation 2.1

We recommend that the Legislative Information Technology office create and maintain a cybersecurity strategic plan.

Recommendation 2.2

We recommend that the Legislative Information Technology office create a detailed incident response plan.

Recommendation 2.3

We recommend that the Legislative Information Technology office create and maintain a more detailed cybersecurity policy.

Recommendation 2.4

We recommend that the Legislative Information Technology office become compliant with a recognizable and accepted cybersecurity standard.

Recommendation 2.5

We recommend that the judicial the branch needs to update and maintain their cybersecurity strategic plan.

Recommendation 2.6

We recommend that the judicial branch ensure that its employees complete the annual cybersecurity awareness training.

Recommendation 2.7

We recommend that the Division of Technology Services work with agencies in the executive branch to ensure that all employees complete the annual cybersecurity awareness training.



Agency Response





Department of Public Safety

JESS L. ANDERSON
Commissioner

State of Utah

SPENCER J. COX
Governor

DEIDRE M. HENDERSON
Lieutenant Governor

May 4, 2023

Kade R. Minchey,
Auditor General

We have reviewed your Exposure Draft of the Performance Audit of the Cybersecurity in the State of Utah (23-24). In the audit, you identified five findings and recommendations relating to the opportunities for government entities to improve cybersecurity readiness, and six finding and recommendations relating to the three branches of government and needed improvements. The Cybersecurity Commission, chaired by Governor Spencer J. Cox and myself, consists of over 45 designated public and private sector individuals with a collective mission to provide recommendations to improve cybersecurity in Utah. We are happy to see that the recommendations from your audit are in line with the Cybersecurity Commission's recommendations provided to the Public Utilities, Energy, and Technology Interim Committee last November. As a result of the hard work of the Commission, many of the recommendations are already being addressed, and we are grateful for the opportunity to use this legislative audit to assist in the Commission's work in 2023.

Below, you will find an acknowledgement and response to each of those findings. The DPS staff and I enjoyed working closely with you and your team on this audit and are appreciative of your hard work and attention to detail. We appreciate the efforts of the Office of the Legislative Auditor General. Auditing cybersecurity in Utah is an incredible undertaking. We are confident that with these findings, DPS can assist the state of Utah to continue to improve the state's cybersecurity posture.

FINDING 1.2 Many entities lack a cyber security framework.

We agree that this audit finding is valid. Using cybersecurity frameworks provides common language and methodologies for managing cybersecurity risk. The Cybersecurity Commission recommends that entities adhere to the NIST Cybersecurity Framework, and recommend the CIS Critical Security Controls and Cyber Hygiene guide as a starting point for maturity models. With this audit's findings, and the additional Commission's recommendations, DPS will continue to encourage entities to adhere to the NIST Cybersecurity Framework.

FINDING 1.2 IT personnel lack the communications skills to accurately present their ideas to management.

We agree that this audit finding is valid. Structured process and procedures assist in alleviating communication issues, but the Department of Public Safety also recommends to invest in workforce

development to also support a culture of strong cybersecurity communication within entities The Department of Public Safety's Statewide Information & Analysis Center will look to find new ways to support IT personnel with information that can aid in presenting cybersecurity topics to management.

FINDING 1.2 Many entities do not require cyber security awareness training.

We agree that this audit finding is valid. The Department of Public Safety requires all of its staff to complete a cybersecurity training and be tested on the training annually. This training is a coordinated presentation with our Statewide Information & Analysis Center cybersecurity staff and the Division of Technology Services. We have found great improvements in our cybersecurity through the implementation of this training and recommend the requirement of this training for all state employees.

FINDING 1.3 Many entities need to improve their cybersecurity compliance with the CIS controls.

We agree that this audit finding is valid. The CIS controls are a great starting point to improve not only cybersecurity compliance, but overall security posture. Implementation of CIS controls minimizes the risk of data breaches, data theft, and many other cyber threats. The Department of Public Safety will continue to find to ways to assist entities abilities towards compliance with the CIS controls.

FINDING 1.4 Many entities lack an incident response plan.

We agree that this audit finding is valid. Incident response plans allow entities to mitigate the risk to cyber-attacks, and enhance preparedness and response. Well thought-out and practiced plans allow for entities to effectively respond to cyber incidents, which are more crucial now with the prevalence of cyber-crimes such as ransomware. Recent legislation in Utah requires the newly codified Cyber Center to collaborate and leverage the Division of Emergency Management to assist with updating and providing best practices to the state's cyber incident response plan. The Department of Public Safety will work to ensure these response plans are leveraged in the coming years to best support cybersecurity for the state of Utah.

FINDING 2.1 A cybersecurity strategic plan will reduce the risk of threats to an entity's infrastructure.

We agree that this audit finding is valid. The Department of Public Safety agrees that a cybersecurity strategic plan reduces the risk of cyber threats and acts as a roadmap for the entity in improving their cybersecurity posture.

FINDING 2.1 Creating a response plan is essential to reduce costs associated with successful cyberattacks.

We agree that this audit finding is valid. Many entities do not have a plan, or have not updated their plan in years. It is recommended to regularly update incident response plans and regularly hold multi-agency exercises to ensure it works as planned. Recent legislation in Utah requires the newly codified Cyber Center to collaborate and leverage the Division of Emergency Management to assist with updating and providing best practices to the state's cyber incident response plan. The Department of Public Safety will work to ensure these response plans are leveraged in the coming years to best support cybersecurity for the state of Utah.

FINDING 2.1 Cybersecurity policies are not robust enough to provide adequate guidance. We agree that this audit finding is valid. While this finding is specific to the Legislature Information Technology office, policies involving cybersecurity are often outdated with how fast technology advances. All entities should update policy on a regular basis to align with cybersecurity best practices, updated incident response plans, and updated strategic plans. The Department of Public Safety will leverage the Cybersecurity Commission to identify and provide adequate guidance surrounding policies for entities.

FINDING 2.1 Legislative Information Technology office needs become compliant with cybersecurity standards.

We agree that this audit finding is valid. Following best practices and cybersecurity standards will reduce risk to cyber-attacks.

FINDING 2.2 Current cybersecurity plan has not been updated since 2014.

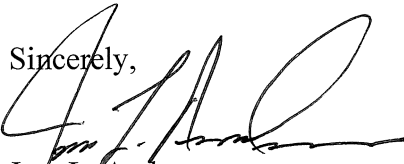
We agree that this audit finding is valid. The Department of Public Safety agrees that a cybersecurity strategic plan reduces the risk of cyber threats and acts as a roadmap for the entity in improving their cybersecurity posture. Recent legislation in Utah requires the newly codified Cyber Center to collaborate and leverage the Division of Emergency Management to assist with updating and providing best practices to the state's cyber incident response plan. The Department of Public Safety will work to ensure these response plans are leveraged in the coming years to best support cybersecurity for the state of Utah.

FINDING 2.2 On average, less than 50 percent of employees are completing annual cybersecurity training.

We agree that this audit finding is valid. Most malware and cyber-attacks stem from phishing emails, which all employees are subject to every day. Remote work adds an added challenge of employees sometimes using personal devices to complete work in some agencies. Every employee is the first step in mitigating risk, as they are the ones initially targeted by cyber criminals. All employees should know common tactics used by cyber criminals and how they can help stop cyber-attacks. The Department of Public Safety requires all of its staff to complete a cybersecurity training and be tested on the training annually. This training is a coordinated presentation with our Statewide Information & Analysis Center cybersecurity staff and the Division of Technology Services. We have found great improvements in our cybersecurity through the implementation of this training and recommend the requirement of this training for all state employees.

Our work enhancing Utah's cybersecurity posture is never complete and we are always looking for ways to improve. I appreciate the great partnership.

Sincerely,



Jess L. Anderson
Commissioner





Utah State Legislature

State Capitol Building | Salt Lake City, UT 84114

May 5, 2023

Kade R. Minchey
Legislative Auditor General
W315 State Capitol Complex
Salt Lake City, UT 84114

Dear General Minchey:

On behalf of all the offices of the Utah State Legislature, as current chair of our administrative oversight body, the Legislative Services Management Council (LSMC), I write to thank you for your team's careful analysis contained in "A Performance Audit of Cybersecurity in the State of Utah." The members of LSMC agree whole-heartedly with your staff's thoughtful recommendations and we have already begun implementing them.

We look forward to working with you and your staff directly as we strive to increase and improve cybersecurity in the legislative branch.

Sincerely,

A handwritten signature in blue ink, appearing to read "Jonathan C. Ball", is written over the typed name and title below.

Jonathan C. Ball
Legislative Fiscal Analyst
2022-2023 Chair
Legislative Services Management Council





Department of Government Operations
Division of Technology Services

State of Utah

SPENCER J. COX
Governor

DEIDRE M. HENDERSON
Lieutenant Governor

MARVIN L. DODGE
Executive Director

ALAN FULLER
Chief Information Officer

May 5, 2023

Kade R. Minchey CIA, CFE
Auditor General
Office of the Legislative Auditor General
P.O 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 Cybersecurity in the State of Utah (23-04). We appreciate the professionalism of you and your staff during this review and for the guidance and recommendations you have provided for improvement. We believe our combined efforts will result in improvements that will benefit the agencies we serve.

We concur with all recommendations in this report and have provided a summary of our actions and timelines to implement the recommendation. The Division of Technology Services/Department of Government Operations is committed to improving protection against cybersecurity threats. We value the insight this audit has provided and look forward to implementing solutions for improvement.

Sincerely,

A handwritten signature in black ink, appearing to read "Marvin L. Dodge".

Marvin L. Dodge
Executive Director
Department of Government Operations

Recommendation 2.1

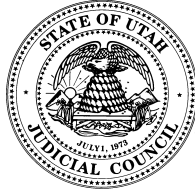
We recommend the Division of Technology work with agencies to ensure all employees complete the annual cybersecurity awareness training.

Division Response: The division concurs.

What: The division will work with the Cabinet Security Council and state agencies to ensure all employees complete the annual cybersecurity awareness training.

How: The Cabinet Security Council meets quarterly and has representatives from state agencies to discuss cybersecurity issues and provide recommendations for improvements, including statewide policies for employees. The division will request guidance and input on how to enforce the requirements of the current policy, and address this issue going forward.

When: The division will discuss this with the Cabinet Security Council at the next quarterly meeting, and will request guidance and recommendations from the Council on how to address this issue.



Administrative Office of the Courts

Chief Justice Matthew B. Durrant
Utah Supreme Court
Chair, Utah Judicial Council

May 1, 2023

Ronald B. Gordon, Jr.
State Court Administrator
Neira Siaperas
Deputy State Court Administrator

Kade Minchey, CIA, CFE
Auditor General
Office of the Legislative Auditor General
W315 State Capitol Complex
Salt Lake City, UT 84114

Dear Mr. Minchey:

Thank you for the opportunity to respond to “A Performance Audit of Cybersecurity in the State of Utah”. The Administrative Office of the Courts (AOC) appreciates you and your staff for reviewing risks for cyberattacks. This audit will help the AOC to better mitigate risks. The AOC supports both recommendations and we are working to implement them as outlined below.

(1) We recommend the Judicial Branch create and maintain a cybersecurity strategic plan.

The 2014 cybersecurity plan of the judicial branch will be updated to help reduce security gaps, extend visibility into security threats, and meet compliance requirements. AOC-IT Department and internal administrators will work with the Judicial Council’s Policy, Planning and Technology Committee to develop recommended changes to the plan. The Judicial Council will provide final approval. AOC-IT will review this plan annually. In addition, the five security related policies that are in draft form will be finalized following the same process.

(2) We recommend the Judicial Branch ensure their employees complete the annual cybersecurity awareness trainings. AOC-IT has started creating a cyber security training that is more aligned with the technology utilized by the courts and the tools we use. This module will be available through our Learning Management System (LMS), and all staff will be required to complete the training yearly. The training will be closely monitored for completion by the AOC Education Department.

The AOC is committed to making the improvements needed to increase protection against cyberattacks and ensure employees complete the required training.

Respectfully,

A handwritten signature in blue ink, appearing to read "Ronald B. Gordon, Jr.", is written over a light blue background.

Ronald B. Gordon, Jr.
State Court Administrator

The mission of the Utah judiciary is to provide the people an open, fair,
efficient, and independent system for the advancement of justice under the law.





Office of the Legislative Auditor General

Olag.utah.gov