CoSN

Leading Education Innovation

2025 STATE CYBERSECURITY LEGISLATION REPORT

CoSN.org

Contents

CoSN
Leading Education Innovation

CoSN's Mission:

CoSN provides current and aspiring K-12 education technology leaders with the community, knowledge, and professional development they need to create and grow engaging learning environments.

www.cosn.org

For access to this report, please visit
www.cosn.org/cybersecurity

I'm pleased to share with you the **2025 State Cybersecurity Legislation Report**, CoSN's latest policy report exploring how state lawmakers are stepping up to protect schools in the face of growing cyber threats.

In 2025, school districts continue to face increasingly complex and costly cybersecurity challenges—yet most remain under-resourced and underprepared. As this report shows, while federal support is shrinking, several states are advancing innovative, bipartisan legislation to help safeguard student data, improve incident response, expand insurance access, and build the cybersecurity workforce we urgently need.

This analysis highlights the legislative activity in Arkansas, Massachusetts, Oregon, Pennsylvania, and Texas—not just to inform, but to inspire. These states represent a range of governance models and policy contexts, yet their common strategies offer actionable ideas for state and district leaders across the country. Our goal is to equip the education community with insights that move us from reactive to resilient.

I encourage you to use this report as both a reference and a call to action. Whether you're advocating for resources, updating local policies, or building new partnerships, this report underscores the importance of system-wide collaboration and strategic leadership.

Thank you for your ongoing commitment to securing the future of digital learning.

I also hope you will explore the many public resources that CoSN, the professional association of school system technology leaders/CIO/CTOs, makes available on cybersecurity at www.cosn.org/cybersecurity.

Sincerely,

Keith Krueger
CEO, CoSN

Introduction

Cybersecurity threats to K–12 schools are growing in frequency, sophistication, and cost according to the Cybersecurity and Infrastructure Security Agency and other government and private sector sources. Yet, many school districts remain under-resourced and underprepared. CoSN's 2025 State of Ed Tech report notes that 61% of school districts rely on general funds, not dedicated cybersecurity budgets, to protect their networks and data (CoSN, 2025). The vast majority of current spending (78%) goes toward monitoring, detection, and response, with 44% of districts outsourcing these functions due to cost and staffing limitations. Monitoring is now the most commonly outsourced IT function in K–12, likely due to the difficulty of acquiring and maintaining in-house expertise (CoSN, 2025).

Despite these investments, most education technology leaders do not perceive their school districts to be at high risk for major cyber threats. Only 27% of districts identified phishing as a high risk, with even fewer, just 13% each, flagging unauthorized disclosure of student data or ransomware attacks as major threats (CoSN, 2025). These relatively low risk perceptions may reflect limited capacity to assess cyber threats, and do not account for the value of student data to cybercriminals, which is often more valuable than adult data due to its long-term utility on the black market (CoSN, 2025).

The K-12 cybersecurity landscape is likely to be further complicated by recent federal policy changes and funding cuts, including the Trump Administration's unilateral elimination of federal support for the Multi-State Information Sharing and Analysis Center (MS-ISAC), which had provided free cybersecurity training and coordination support to districts. Without this support, cybersecurity risks are likely to grow, especially in underfunded and understaffed districts (CoSN, 2025).

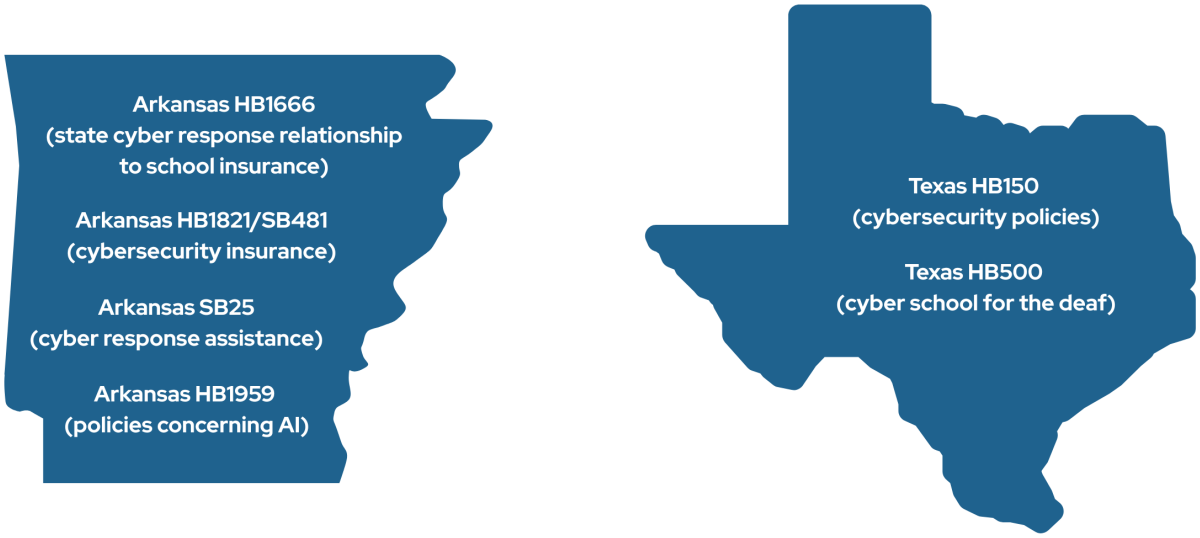
In contrast to troubling recent federal developments, some state policymakers have stepped up this year by introducing cybersecurity legislation and approving new laws that are designed to help school districts. This policy paper highlights legislative developments in five diverse states—Arkansas, Massachusetts, Oregon, Pennsylvania, and Texas—to identify common strategies and actionable insights for other state and local leaders. CoSN selected these states because they represent a range of regional, political, and governance contexts, and their recent activity reflects both mature and emerging state-level responses to K–12 and related education or public sector cybersecurity needs.

By learning from these examples, education leaders and policymakers in all states can better understand what's working, what's emerging, and how to move from fragmented, reactive approaches to systemic, resilient cybersecurity strategies.

Summary of 2025 State K-12 Focused Cybersecurity Legislation

Legislators in Arkansas (6 bills), Massachusetts (5 bills), Oregon (2 bills), and Texas (5 bills) introduced eighteen bills this year focused on improving K-12 cybersecurity. Pennsylvania did not consider any K-12 focused bills. The K-12 focused bills look beyond general government or postsecondary applicability and directly target, in some fashion, school districts, public elementary and secondary schools, education service agencies, or other K-12 institutions. Common policy themes embedded in the eighteen bills include expanding access to cybersecurity insurance, establishing enhanced training and infrastructure support, improving cyberattack responses, standardizing data practices, and requiring cyber risk assessments within K–12 systems.

Of the eighteen K-12 focused cybersecurity bills introduced in the states featured in this paper, seven were enacted but only in two states: Arkansas and Texas.



The remaining twelve bills failed to advance or were still pending as of mid-July 2025. The introduced and enacted K-12 centric bills show that lawmakers in these covered states recognize the need to strengthen schools' cyber readiness and response. A complete list of the eighteen K-12-specific bills (enacted and unenacted) follows in the next section.

K–12 Focused Cybersecurity Bills

Arkansas

Amends existing law relating to the state's cyber response program which includes school districts as participating governmental entities **(HB1666) – Enacted**

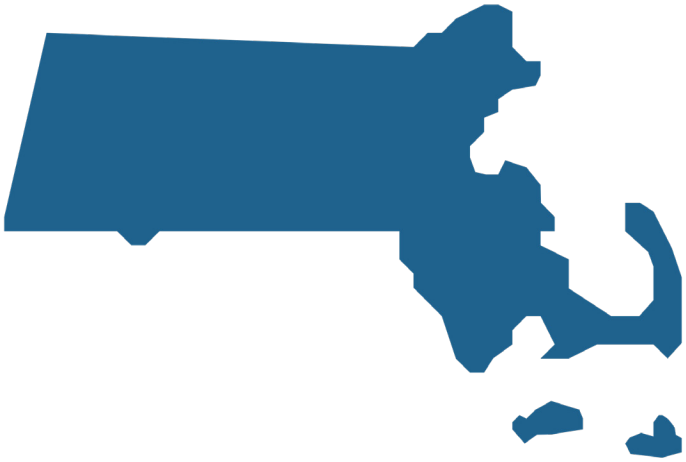
Requires the State Insurance Department to offer cybersecurity insurance for public schools and gives the Department the authority to mandate reporting requirements for districts **(HB1821) – Enacted**

Amends existing policy regarding use of technology resources and cybersecurity by public entities, including public school districts, to require creation of policies concerning the authorized use of artificial intelligence **(HB1959) – Enacted**

Expands the responsibilities of technology coordinators in education service cooperatives to include cyber incident response **(HB2002) – Not Enacted**

Appropriates funding for the Arkansas Self-Funded Cyber Response Program to assist school districts after cyberattacks **(SB25) – Enacted**

Companion to HB1821; also provides cybersecurity insurance coverage requirements for K–12 schools **(SB481) – Enacted**



Massachusetts
Prohibits employers, defined to include school districts, from using electronic monitoring tools to collect employee information - any data collected must be consistent with the state's data and cyber-privacy laws **(H77 & S35) - Pending**

Provides funds to Bellingham Public Schools for cybersecurity infrastructure as part of a larger appropriations bill **(H4227 & S2514) – Pending**

Amends school improvement planning and early education policies to include cybersecurity, privacy, and screen time limitations **(S463) – Pending**

Oregon
Directs the Department of Education to standardize student data practices and analyze cybersecurity risks in K–12 schools **(HB2508) – Pending governor's action**

Companion to HB2508; also addresses cybersecurity in student data systems for school districts and educational service districts **(SB312) – Not Enacted**

Texas
Establishes the Texas Cyber Command in place of the Department of Information Resources - amends the law to make clear that school districts must ensure cybersecurity policies do not conflict with information security standards for institutions of higher education adopted by the Texas Cyber Command; tasked with cybersecurity training, including K–12 systems **(HB150/SB2176) – Enacted**

Provides funds to the School for the Deaf for information technology and cybersecurity initiatives **(HB500) – Enacted**

Requires a state study to identify ways for school districts to improve cybersecurity and address rising costs **(SB1686) – Not Enacted**

Makes cybersecurity programs eligible under the Rural Pathway Excellence Partnership for in-person or remote instruction **(SB2132) – Not Enacted**

The Evolving State Policy Landscape

While the above bills focused more squarely on K–12 education, a broader set of legislative efforts in 2025 showed a strong state-level commitment to strengthening cybersecurity across all public sectors—including postsecondary education, state agencies, and critical infrastructure. Of the 61 total bills (K-12 focused and broader cybersecurity bills) introduced in the five studied states, most measures addressed general government systems, postsecondary institutions, or cross-cutting issues such as insurance, incident response coordination, AI accountability, and statewide workforce development. Many bills referenced multiple sectors (e.g., both K–12 and postsecondary). These broader bills illustrate a trend toward comprehensive cybersecurity governance, with several proposals creating centralized cyber commands, requiring state and local agencies to adopt baseline cyber standards, investing in higher education cybersecurity training programs, and funding response infrastructure accessible to multiple sectors—including schools.

If enacted, many of these broader policy initiatives would benefit the K–12 sector indirectly by:

- Expanding shared cybersecurity services and insurance pools;
- Establishing regional security operations centers and training pipelines involving community colleges and universities;
- Requiring coordinated incident reporting across agencies and municipalities; and
- Creating legal frameworks for data privacy and artificial intelligence accountability.

These developments suggest that states recognize cybersecurity as a systemic issue that spans education, public safety, health, and digital infrastructure. While K-12 systems remain especially vulnerable, they often now sit within a wider legislative push to modernize and secure public sector technology.

These broader legislative trends may also demonstrate a maturing state policy landscape that emphasizes proactive governance, coordinated response infrastructure, public-sector system readiness, and cybersecurity workforce development. While K–12 systems remain a clear area of concern, state leaders are often focused on policies that embed school districts within a larger framework of cyber resilience—often alongside higher education institutions, local governments, and state agencies. This activity reflects several urgent realities:

Persistent Threats: Public-sector institutions, including school districts, continue to be frequent targets of ransomware groups and other cybercriminals, with attacks growing in scale and sophistication.

Federal Encouragement and Support: Guidance and funding from the Cybersecurity and Infrastructure Security Agency (CISA), the State and Local Cybersecurity Grant Program, and emerging federal standards had been catalyzing state-level action but that trend may wane under the current administration's funding cuts.

Capacity Gaps: Many public entities, especially school districts and smaller agencies, still lack dedicated cybersecurity staff, infrastructure, and incident response protocol, prompting states to take on greater roles as policy leaders, conveners, and resource hubs.

Key Legislative Strategies in the Studied States

Several common policy strategies emerged across the cybersecurity legislation introduced or enacted in the tracked states—Arkansas, Massachusetts, Oregon, Pennsylvania, and Texas—in 2025. These strategies reflect a shared focus on improving cyber preparedness, governance, and workforce capacity in both education and broader government systems.

Common Legislative Strategies in 2025

Strategy	States
Centralized Cyber Oversight	AR, MA, PA, TX
Cyber Insurance and Risk Mitigation	AR, MA, OR, TX
Workforce Development and Education	MA, OR, TX
K–12 and Higher Ed Cyber Integration	AR, MA, TX
Incident Reporting and Crisis Response	MA, OR, PA, TX
AI and Privacy-Cyber Integration	AR, MA, TX

Centralized Cybersecurity Governance and Oversight

States are taking more steps to set up central teams to manage cybersecurity, enforce standards, and coordinate responses.

Arkansas HB1549 (Enacted): Established the State Cybersecurity Office with authority over cybersecurity functions across state agencies and designated it as a resource for local governments and educational institutions.

Texas HB150 (Enacted): Created the Texas Cyber Command to lead cybersecurity prevention, response, and coordination across governmental entities.

Pennsylvania HB1219/SB373 (Pending): Proposed the creation of an Office of Information Technology and a Joint Cybersecurity Oversight Committee.

Massachusetts S39 (Pending): Proposed a statewide Cyber Incident Response Team tasked with cross-agency planning and coordination.

Cybersecurity Insurance and Risk Management

States are working to manage cybersecurity liability and financial exposure through insurance frameworks and dedicated funds.

Arkansas HB1821/SB481 (Enacted): Requires all public school districts, education service cooperatives, and charter schools to obtain cybersecurity insurance and gives the State Insurance Department the authority to require each entity to submit program reports.

Oregon HB3228 (Not Enacted): Proposed a Cybersecurity Resilience Fund to support public bodies—especially those unable to meet cyber insurance requirements—via the Cybersecurity Center of Excellence.

Massachusetts H3363 (Pending): Encouraged preference for IT vendors with cybersecurity insurance during state procurement.

Cybersecurity Workforce Development and Education

Many states are investing in career pathways and training infrastructure to address the cybersecurity talent gap.

Massachusetts H3983/H4227 (Pending): Proposed funding for cybersecurity workforce programs, including cyber ranges and scholarships, with a focus on equity and partnerships with community colleges.

Oregon HB3228 (Not Enacted): Directed funding to improve IT systems and enhance cybersecurity readiness across state agencies, with implementation support through the Higher Education Coordinating Commission.

Integration of Cybersecurity into K–12 and Higher Education Policy

States are embedding cybersecurity readiness and risk mitigation policies into the education sector—especially at the district and institutional level.

Arkansas HB1821 (Enacted): Would mandate cybersecurity risk insurance coverage and allows for reporting for public school systems.

Massachusetts S463 (Pending): Would incorporate cybersecurity, privacy, and screen time benchmarks into school improvement plans and require early childhood educator training on digital safety.

Texas SB1686 (Not Enacted): Would require a state study to assess school districts' cybersecurity needs and rising costs.

Incident Reporting and Crisis Response Readiness

There is growing emphasis on incident preparedness, real-time reporting, and ensuring public entities have playbooks for rapid response.

Massachusetts HD4360 (Pending): Would require all municipalities and school districts to report cybersecurity incidents to the state's operations center.

Texas HB3112 (Enacted): Would allow government bodies to discuss cybersecurity policies related to critical infrastructure in closed meetings, enhancing confidentiality during crisis response.

Pennsylvania HB1219 (Pending): Would add situational awareness and threat coordination as core duties of the proposed Office of Information Technology.

AI, Privacy, and Cybersecurity Intersections

States are proactively aligning cybersecurity strategies with emerging technologies like artificial intelligence and digital privacy regulation.

Massachusetts S2516/H104 (Pending): Proposes a comprehensive data privacy framework requiring cybersecurity safeguards and risk-based limits on personal data collection.

Arkansas HB1959 (Enacted): Requires all public entities, including school districts, to adopt policies governing the authorized use of artificial intelligence.

Texas HB1709 (Not Enacted): Would require cybersecurity impact assessments for high-risk AI systems deployed by state agencies.

Policy Recommendations for State and Local Education Leaders

Looking at the cybersecurity measures introduced this year in the five studied states, we recommend that state and local leaders consider adopting policies and practices across a number of areas including improving governance, funding risk assessments, expanding the cybersecurity workforce, requiring reporting and response readiness, and modernizing procurement and data standards. In each of these areas, policymakers should consider K-12 schools' cybersecurity needs and aim to address them.

Establish or Strengthen Statewide K–12 Cybersecurity Governance

Recommendation: Designate a cybersecurity lead within the state education agency and ensure that school districts are included in state-level cybersecurity planning and governance bodies.

State Examples:

Arkansas enacted multiple bills in 2025 including one that centralized cybersecurity oversight in a newly empowered State Cybersecurity Office **(HB1549).** This office is responsible for setting statewide policies, including those that impact school districts.

Texas created the Texas Cyber Command **(HB150)**, a centralized structure charged with coordinating prevention, detection, and response for cybersecurity incidents across government—including education systems.

Pennsylvania introduced legislation to establish an Office of Information Technology and a Joint Cybersecurity Oversight Committee **(HB1219, SB373)**, which would guide statewide cybersecurity governance and coordinate policy across agencies, including education.

Fund and Require School District Cybersecurity Risk Assessments

Recommendation: Allocate funding for school districts to conduct risk assessments and develop mitigation strategies. Consider state-run insurance pools or financial support mechanisms.

State Examples:

Arkansas enacted legislation **(HB1821/SB481)** requiring school districts to report on their cybersecurity insurance status and authorized the State Insurance Department to manage a program covering district cybersecurity risks.

Oregon proposed the Cybersecurity Resilience Fund **(HB3228)**, which would help public bodies, including school districts, afford insurance and address security gaps.

Texas included cybersecurity risk and insurance reviews in bills requiring evaluations of agency IT systems **(HB1500, SB2404)**, laying groundwork for broader assessment programs.

Align Workforce Policy with K–12 Needs

Recommendation: Support teacher certification in cybersecurity and create K–12 student pathways aligned with current and emerging workforce demand.

State Examples:

Massachusetts introduced legislation to invest in cybersecurity workforce development, including funding for cyber ranges, scholarships, paid internships, and public awareness campaigns **(H3983, S49).**

Texas passed or introduced several bills **(HB1527, SB2097, SB2132)** including measures to expand tuition exemptions and career pathway programs to include students and educators in cybersecurity-related fields.

Oregon legislation **(HB3228)** would fund training through the Cybersecurity Center of Excellence, targeting both public agencies and education partners.

Mandate Incident Reporting and Create Response Protocols

Recommendation: Require timely reporting of cybersecurity incidents and support districts with coordinated response plans and training exercises.

State Examples:

Massachusetts introduced legislation **(HD4360)** requiring cities, towns, and school districts to report known cybersecurity incidents to the Commonwealth's Security Operations Center.

Texas passed **HB3112**, permitting governmental bodies—including school boards—to deliberate on cybersecurity matters in closed session, helping them develop response plans without exposing sensitive information.

Arkansas updated its Freedom of Information Act **(SB227)** to allow executive sessions for discussing cybersecurity breaches.

Update Procurement and Data Governance Standards

Recommendation: Require that vendors meet minimum cybersecurity standards and align procurement processes with national frameworks (e.g., NIST, CIS).

State Examples:

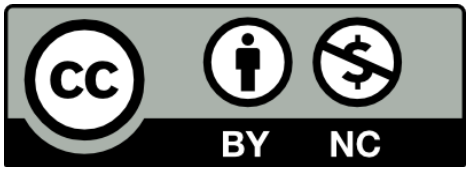
Massachusetts considered legislation **(H3363)** requiring state agencies, including those procuring education technology, to give preference to vendors that carry cybersecurity insurance—helping enforce a security baseline through procurement.

Texas passed **HB5331**, ensuring that no contract language in cybersecurity or IT service contracts can restrict a public entity's compliance with state cybersecurity law—effectively preventing vendors from blocking governance or enforcement.

Oregon considered legislation **(HB2508, SB312)** would require education agencies to standardize data governance practices, with attention to cybersecurity risks in the handling of student data.

Conclusion

State and local education leaders face mounting pressure to secure digital learning environments against increasingly sophisticated cyber threats. The 2025 legislative actions reviewed in this paper provide ideas for developing and adopting policies that will help school districts and their partners address this challenge. By adopting well designed strategies – centralized oversight, insurance requirements, workforce investment, integrated planning, and responsible innovation oversight– states can help their school districts move from reactive to resilient. Cross-sector collaboration and sustained investment will be critical to protecting students, educators, and the integrity of public education systems. For further information, please visit CoSN's website to review our Cybersecurity Project's many related cybersecurity resources.



CoSN
Leading Education Innovation