Cybersecurity Governance in California K-12 School Districts: The Cost of Federal Cuts and the Case for State Action

Seung Yeon (Sunny) Lee
May 15, 2026

Introduction

K-12 school districts are prime targets for cyberattacks. According to the Center for Internet Security (CIS), 82% of roughly 5,000 reporting K-12 schools experienced cyber attacks nationally, with at least 9,300 confirmed incidents recorded during that period.[1] Ransomware, phishing, and data breaches exposing sensitive student and staff records have now become routine threats. However, school districts continue to operate with chronically limited internal capacity: understaffed IT teams, no dedicated cybersecurity budgets, and no standardized requirements for preparedness.

Several federal funding cuts in 2025 considerably worsened this gap. To illustrate, the Multi-State Information Sharing and Analysis Center (MS-ISAC), which was the only federal program providing free real-time cybersecurity services to districts regardless of size, was defunded in September 2025 and converted to a paid model.[2] Beyond MS-ISAC, the Office of Educational Technology, the sole federal office providing K-12 cybersecurity policy guidance, was eliminated in March 2025; the K-12 Government Coordinating Council was paused less than a year after its creation.

In light of these events, this capstone project, partnered with the Consortium for School Networking (CoSN), conducted a study on cybersecurity governance in California K-12 school districts.[3] Specifically, it asks two questions: what operational and financial consequences have California districts experienced following the 2025 federal funding disruptions (particularly the defunding of MS-ISAC), and what structural profiles of financial vulnerability and organizational capacity characterize California districts today? It draws on a structured survey of 43 California K-12 technology leaders conducted in Spring 2026 to assess both the immediate impact of the 2025 cuts on California districts and the underlying organizational conditions that made them vulnerable in the first place. Ultimately, the study aimed to inform state-level policy responses tailored to California's institutional landscape.

Key Findings

Finding 1: The MS-ISAC funding cuts made districts feel less secure.
Among the 27 California K-12 districts that had actively used MS-ISAC, overall perceived security declined significantly after the September 2025 funding cuts (a statistically significant drop). Two-thirds

[1] "2025 CIS MS-ISAC K-12 Cybersecurity Report: Where Education Meets Community Resilience," *Center for Internet Security*, March 6, 2025, https://www.cisecurity.org/insights/white-papers/2025-k12-cybersecurity-report.
[2] Free MS-ISAC services have since been restored for some states, including California.
[3] The full methodology, survey instrument, and statistical analysis are available in the complete capstone report.

reported that previously manageable threats had escalated in priority, with the loss of real-time threat intelligence as a primary driver.

Finding 2: Financial constraints, observed following the MS-ISAC funding cuts, are tangible.
Following MS-ISAC funding cuts, 58% of all surveyed districts reported that their ability to fund cybersecurity declined over the past year. MS-ISAC users were nearly twice as likely to report funding changes as non-users (70% vs. 38%), reflecting the direct cost of replacing previously free services.

Finding 3: The governance typology reveals a systemic gap.
A four-quadrant governance typology that maps districts by external financial vulnerability and internal organizational capacity reveals the structural landscape.

- **30% (13 districts) are "Most Vulnerable."** They possess high financial vulnerability and low organizational capacity, lacking both the resources and the internal infrastructure to respond to threats independently.
- **37% (16 districts) are "Underperforming."** They possess lower financial vulnerability but still weak organizational capacity. Districts in this quadrant have relatively stable finances, yet have not built basic preparedness infrastructure, suggesting the problem is not resources but the absence of any external mandate requiring them to act.
- **Only 5% (2 districts) are "Constrained but Capable."** They possess high financial vulnerability but strong organizational capacity. The rarity of this group may perhaps be a reflection of what the current governance architecture produces.
- **28% (12 districts) are "Best Positioned."** They exhibit both financial stability and strong internal capacity, though interview evidence suggests this status typically resulted from internal crises that forced investment rather than from any external requirement or standard.

Recommendations for California Policymakers

1. **Establish a State-Level Cybersecurity Monitoring Mechanism**

Require all California K-12 districts to submit an annual self-assessment of cybersecurity organizational conditions (staffing, budget, incident response, and planned actions) to the California Cybersecurity Integration Center (Cal-CSIC) or the California Department of Education. Individual reports should remain confidential; aggregate statewide data should be published to reinforce accountability. Without this baseline, policymakers cannot target interventions or measure progress.

2. **Mandate Minimum Cybersecurity Standards**

Establish a baseline floor every district must meet, regardless of size or resources. This may include a designated cybersecurity accountability role, a written incident response plan reviewed annually, and at least one facilitated tabletop exercise per year with leadership. Legislation should define minimum cyber hygiene controls (e.g., multi-factor authentication, regular patching, phishing awareness training) with a phased implementation timeline to ensure compliance is achievable.

3. **Build Internal Capacity Through County Offices of Education**

Route state-supported capacity-building through county offices of education, which already have administrative relationships with every district in their jurisdiction. Each county office should be resourced to provide districts with standardized templates for incident response plans, facilitated tabletop sessions, and structured governance councils connecting technology directors with district leadership.

The withdrawal of federal cybersecurity support exposed a structural vulnerability that California's current legislative framework cannot address on its own. Without systematic data on district cybersecurity capacity, the state cannot effectively target support where it is most needed. This study hopes to provide that baseline by offering California policymakers an empirical foundation for state action.

About the Research

This brief is drawn from "Cybersecurity Governance in California K-12 School Districts: A Survey-Based Assessment" (Seung Yeon Lee, Goldman School of Public Policy, UC Berkeley, Spring 2026), submitted in partnership with the Consortium for School Networking (CoSN). The full report includes the complete survey instrument, variable construction, sensitivity analyses, and governance typology methodology. Findings are based on 43 completed survey responses from California K-12 technology leaders.