

OPERATIONAL AI IN EDUCATION:

Readiness, Realities, and the Road Ahead

A CoSN 2026 MEMBER SURVEY



OPERATIONAL AI IN EDUCATION:

Readiness, Realities, and the Road Ahead

Building on the foundation of our 2025 membership survey, the 2026 report examines how K-12 school districts leverage artificial intelligence (AI) across operational domains. In this second edition, we not only track how these operational realities have evolved over the past year, but also shift the focus from AI adoption inside network environments to AI governance and cybersecurity.

A special thanks to HPE for making this report possible, with their support we continue to understand and champion the needs of school districts in this quickly evolving environment.

Methodology

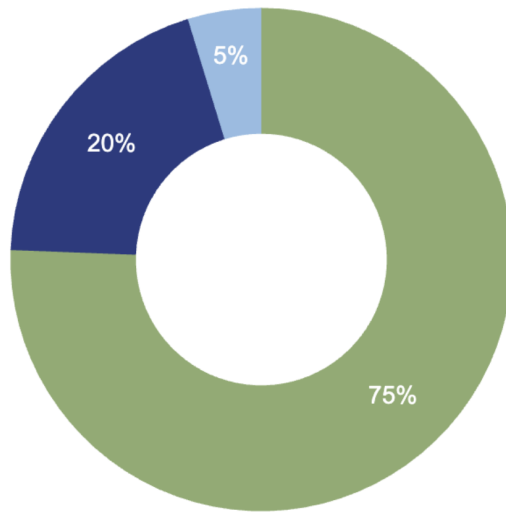
Our research partner, FullScale, conducted a short survey between August 11–28, 2026. Based on responses from 192 CoSN members (as compared to 281 in 2025), the survey results provide insights into the priorities, barriers, and opportunities that are top-of-mind for our members. When reviewing the year-over-year comparisons, keep in mind that fewer respondents completed this year's survey.

Demographics

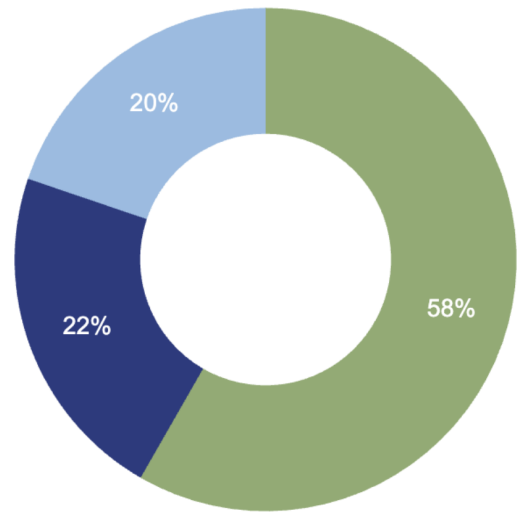
The demographics of the survey respondents do not fully mirror CoSN's overall membership, so findings should be taken as descriptive and not representative. Across the membership, 75% of districts classify themselves as rural or town, 20% suburban, and 5% city. Among survey respondents, 58% identify as suburban, 22% as urban, and 20% as rural.¹

¹ Part of this gap may reflect how the two figures have been produced. Membership locale is assigned using federal classifications, while survey respondents characterized their own districts. Findings should be read as a reflection of districts that responded, not as representative of the full CoSN membership.

CoSN Membership Geography



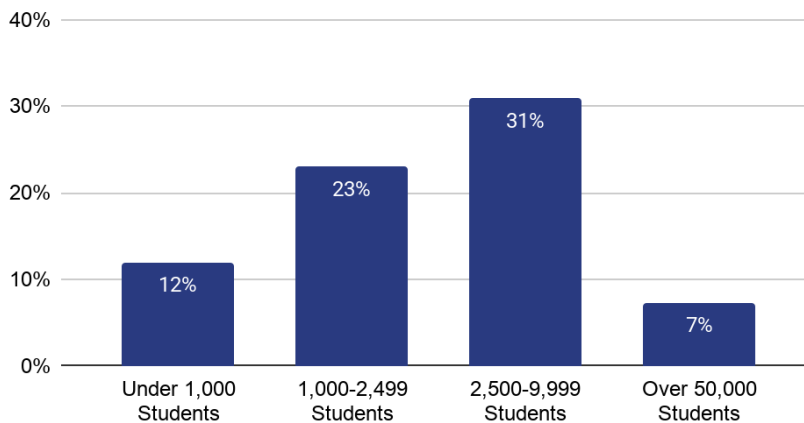
Survey Respondent Geography



● Rural or Town ● Suburban ● City

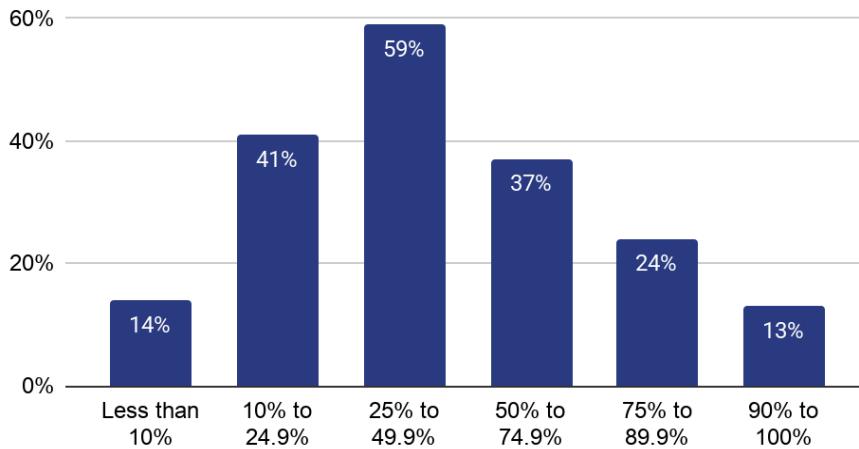
When looking at the survey respondents by student enrollment, the largest single group of districts fell in the 2,500–9,999 student range (31%), followed by districts of 1,000–2,499 students (23%); districts at either extreme — under 1,000 students or over 50,000 — were represented as 12% and 7% respectively.

Survey Respondent Reported District Enrollment



Free-and-reduced-price-meal eligibility was more evenly spread across the sample: the single most common band was 25%–50% of students qualifying (31%). Every bracket from under 10% to over 90% was represented with the majority (59%) reporting that 25–49.9% qualify for nutritional support.

Reported Free-and-Reduced-Price-Meal Eligibility



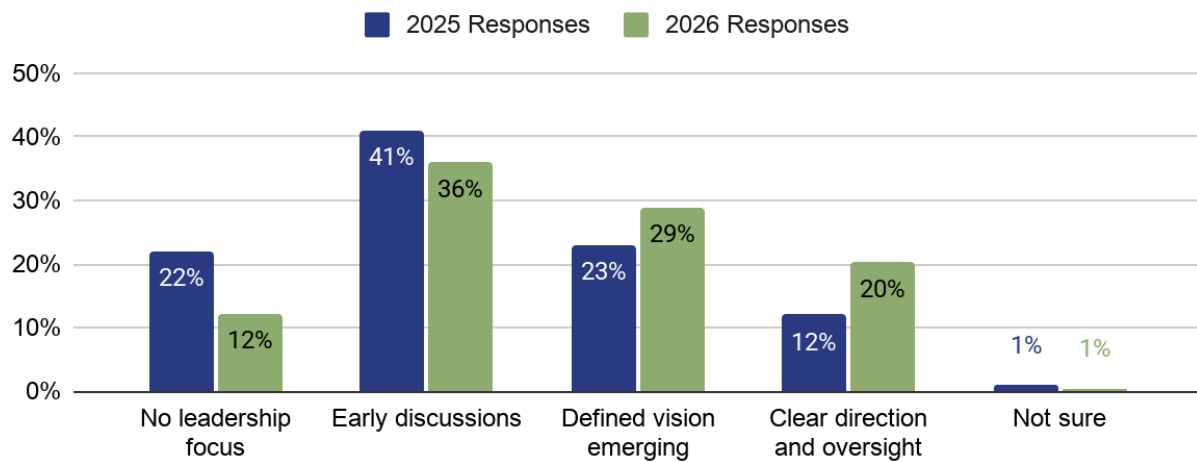
Progress Since 2025

The survey repeated five questions from the 2025 survey to identify potential progress in terms of reported leadership in setting direction on AI, confidence with cybersecurity, legal and compliance review, as well as IT and academic team readiness. The data indicate that respondents perceive that they have made progress over the last year.

Leadership Direction Setting

Approximately 20% of districts now report that their leadership has set clear direction and oversight for AI, nearly double the 12% reported in 2025. Additionally, the percentage of respondents who previously indicated a lack of leadership focus decreased substantially from 22% to 12%. While there has been a shift in districts making progress on their direction setting, it is worth noting that the majority of districts, approximately 66%, report that they are still in *early-discussion* or *vision forming* stages.

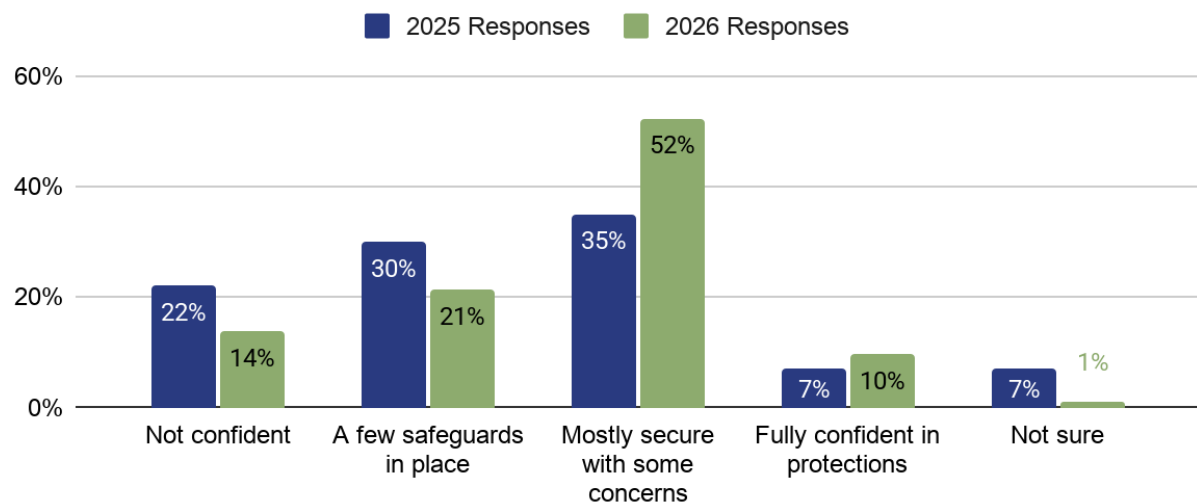
How actively is your district's leadership setting direction for the use of Generative AI in operational areas (e.g., HR, finance, facilities, transportation)?



Cybersecurity Readiness

Respondents indicated increased confidence in their cybersecurity readiness. In 2026, those that claimed to feel *mostly secure with some concerns* jumped from 35% to 52%, and those with no confidence fell from 22% to 13%. However, those that felt *fully confident* remained consistent.

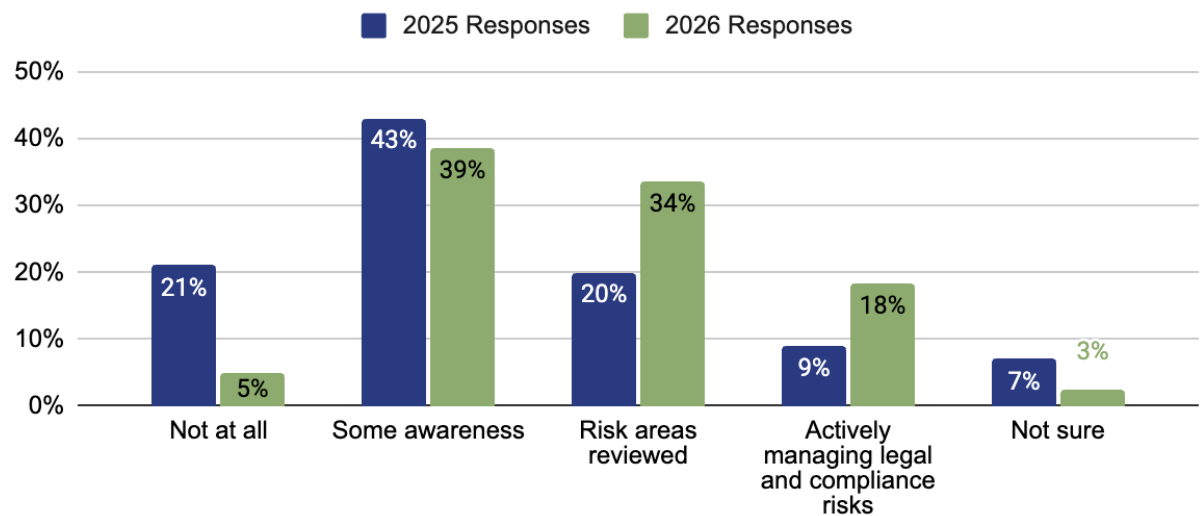
How confident are you that your district's use of Generative AI is aligned with cybersecurity best practices?



Legal and Compliance Readiness

Since last year, districts that had *not at all* considered legal or compliance risks associated with Generative AI use dropped from 21% to 5%. At the same time, those *actively* managing legal and compliance risks nearly doubled. Those who have at least considered specific risk areas increased from 20% to 34%.

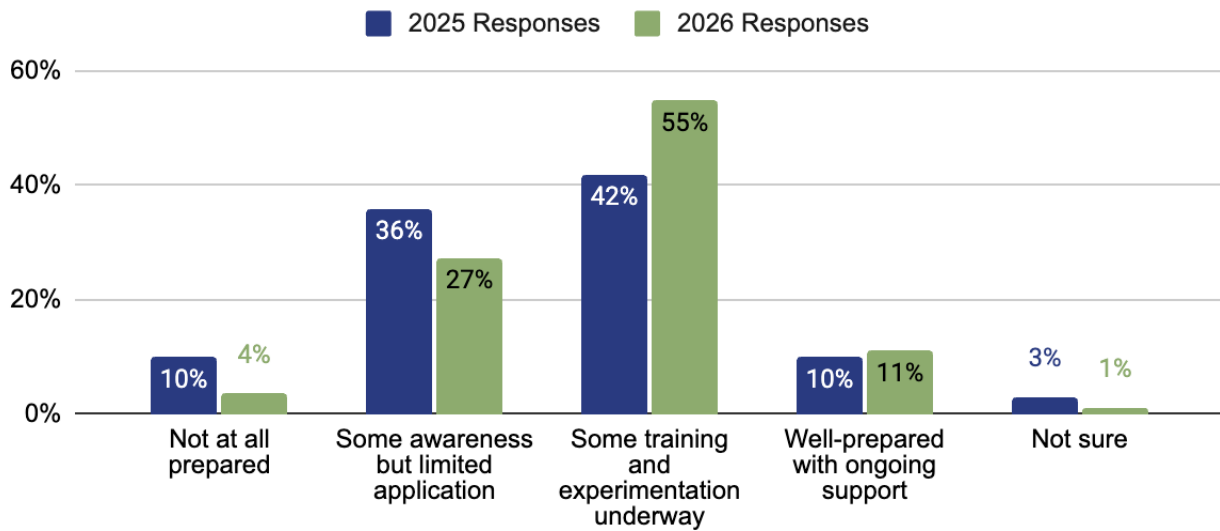
Has your district considered legal or compliance risks related to Generative AI use?



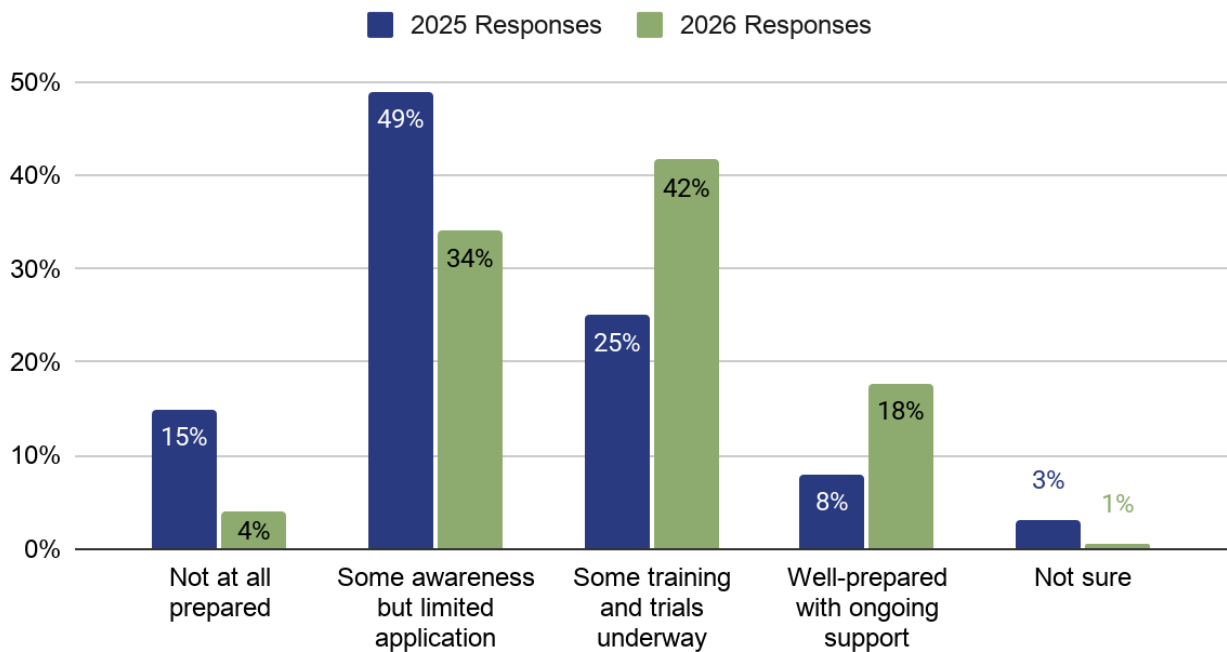
AI Literacy Readiness: Academic and IT Staff

The 2026 data indicates a notable shift in how academic and IT readiness compare. Over half of the respondents (56%) indicated that their districts have training and experimentation underway for academic staff, but relatively few have progressed to full, ongoing support. However, districts indicated increased readiness among their IT staff. For districts weighing where to direct professional development resources, this distinction is worth noting. Academic teams may benefit most from more entry-level professional learning, while IT teams may be ready for deeper, more sustained investment.

How prepared are educators in your district to integrate Generative AI into instruction?



How ready is your district's IT workforce with the education and knowledge needed to support AI operations?



2026 District Reported Priorities

To understand where districts may be focusing their efforts over the next two years, the 2026 survey asked respondents to rank nine technology priorities from most to least important: AI governance, cloud modernization, cybersecurity, device management, digital equity, disaster recovery, network modernization, student data privacy, and staff training. All 192 respondents completed the full ranking.

Cybersecurity emerged as the top priority. More than half of districts (57%) ranked it their single highest priority, and approximately 83% placed it in their top three. This finding is in alignment with the [2026 Driving K-12 Innovation Report](#) as ensuring cybersecurity emerged as one of the top hurdles to address. Cybersecurity presents a unique challenge for districts in that it involves human capacity, policy, as well as ongoing training and monitoring in addition to technical safeguards.

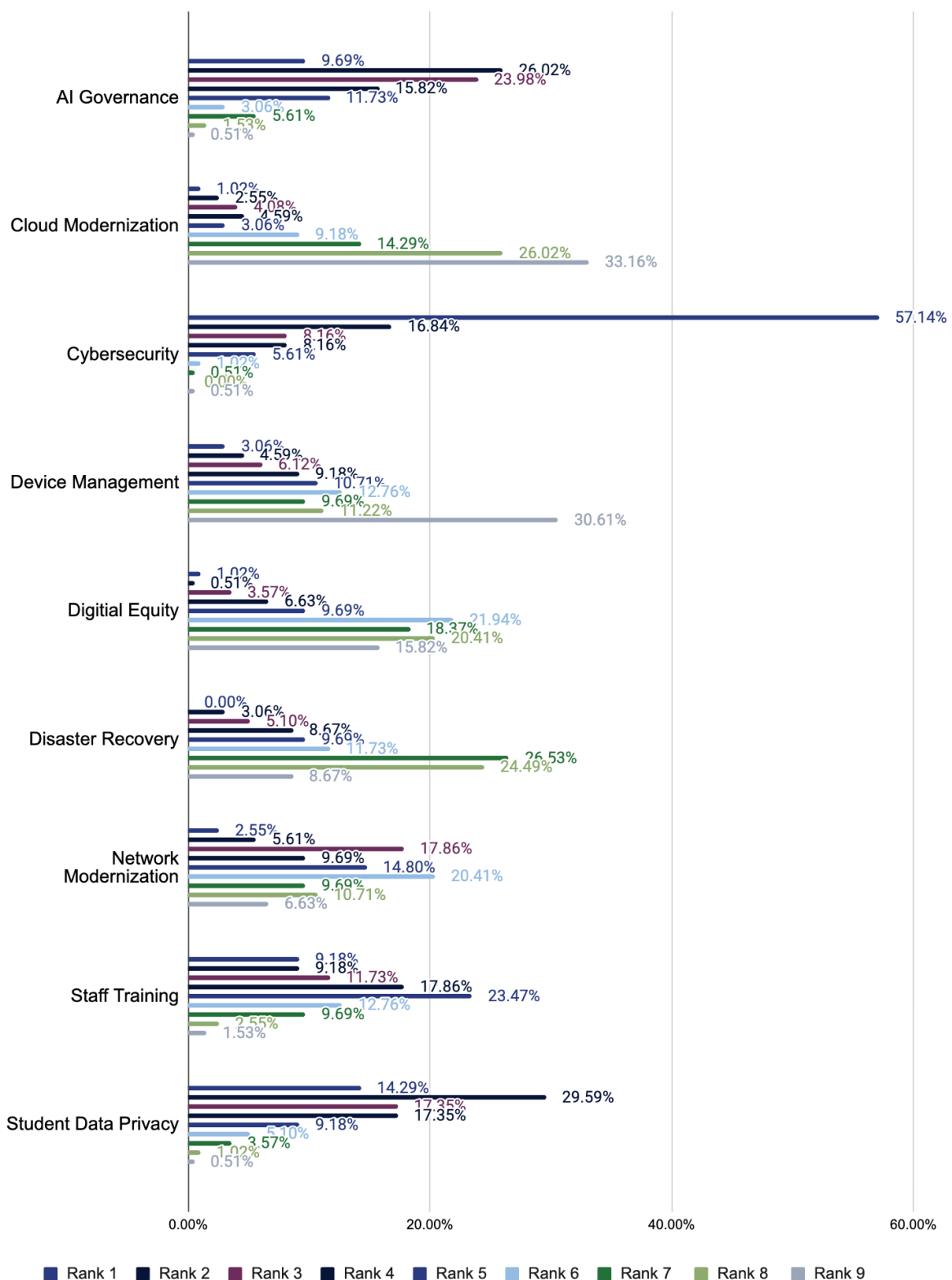
Student data privacy and AI governance also emerged as top priorities in the data. Relatively few districts (10%) ranked AI governance as their single top priority, but 26% placed it second and 24% ranked it third.

Staff training and network modernization form a distinct third tier indicating a common mid-list pick rather than a frequent top choice. The remaining four priorities (device management, disaster recovery, digital equity, and cloud modernization) form a clear bottom tier, each with fewer than 15% of districts placing them in the top three. Disaster recovery was never ranked first, and yet was not consistently ranked last either, suggesting it is rarely urgent but also rarely dismissed.

For CoSN members setting priorities for the next 24 months, the data point to a fairly clear read: cybersecurity and AI governance present two key issues to address.

The figure on the following page presents a comparison of the rankings across the nine different technology priorities.

What are your district's top technology priorities for the next 24 months?



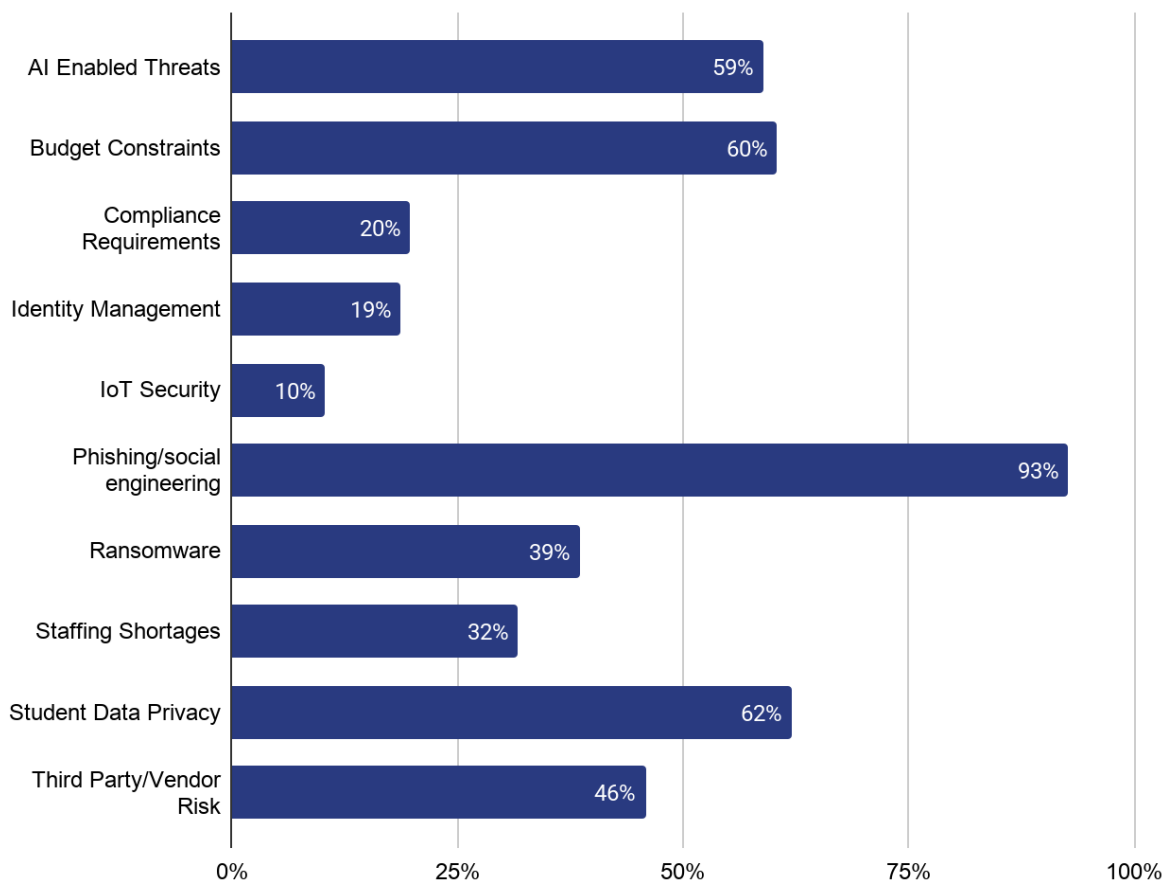
Cybersecurity

Recognizing that cybersecurity presented a unique challenge for CoSN members, the survey asked several additional questions.

Top Challenges

Respondents were asked to select up to five cybersecurity challenges, from a list of 10, that they perceive create the greatest risk for their district. Phishing and social engineering was the most commonly indicated risk as 93% of individuals included it in their list. Three challenges clustered closely behind it: student data privacy (62%), budget constraints (60%), and AI-enabled threats (59%). Ransomware, despite being the specific incident type named in the recovery-readiness question below, ranked sixth.

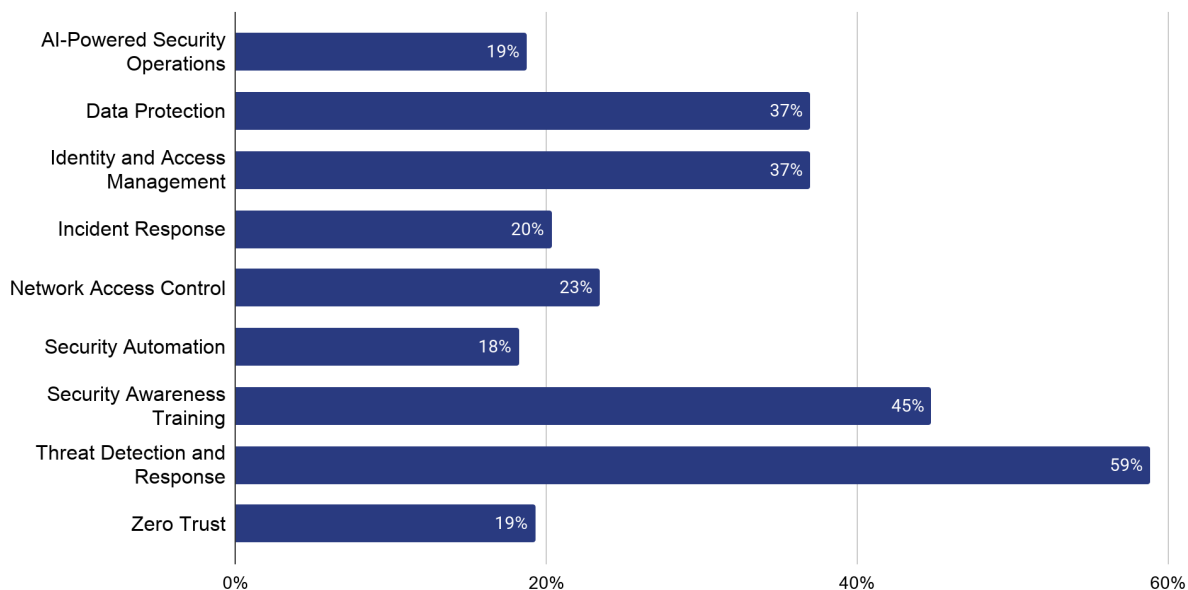
What cybersecurity challenges create the greatest risk for your district?



Investment Priorities

To understand where districts plan to invest over the next two years, respondents could choose up to three items from a list of nine. Respondents indicated that their districts intend to prioritize *threat detection and response* (58%), followed by *security awareness training* (45%). These responses align with the challenges noted above, as awareness training offers a direct countermeasure to phishing and social-engineering risks. Identity and access management as well as data protection were each selected by 37% of respondents. Newer, more specialized categories such as AI-powered security operations (19%) and security automation (18%), sit at the bottom of the list, suggesting that these may be more emerging investments rather than near-term priorities.

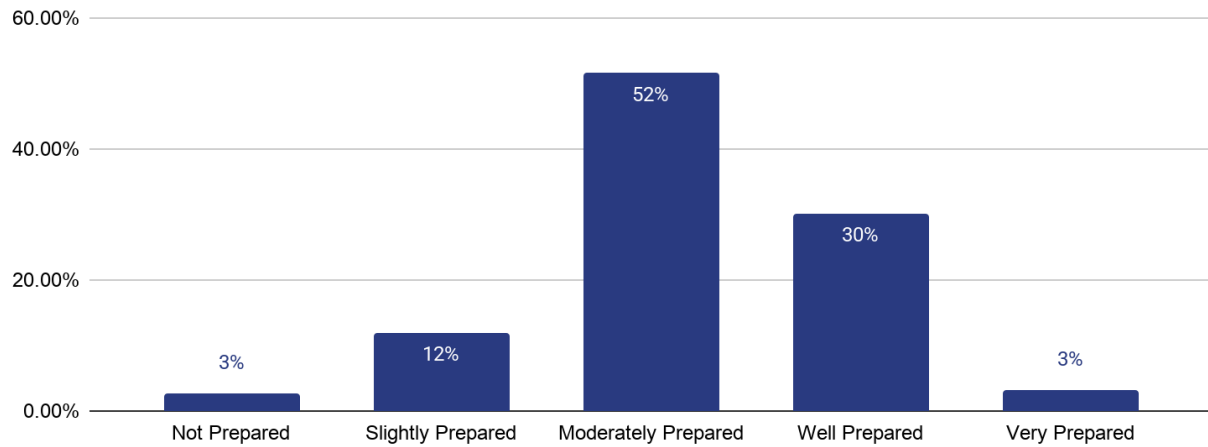
What security capabilities are your highest investment priorities over the next two years?



Incident Recovery Readiness

Respondents were directly asked how prepared they felt to recover from a ransomware or cybersecurity incident. Nearly half (52%) describe themselves as *moderately prepared*, with 30% *well prepared* and only 3% *very prepared*. In contrast, 14% describe themselves as either *not prepared* or *only slightly prepared*. Overall, very few districts feel either *not prepared* or *very prepared*.

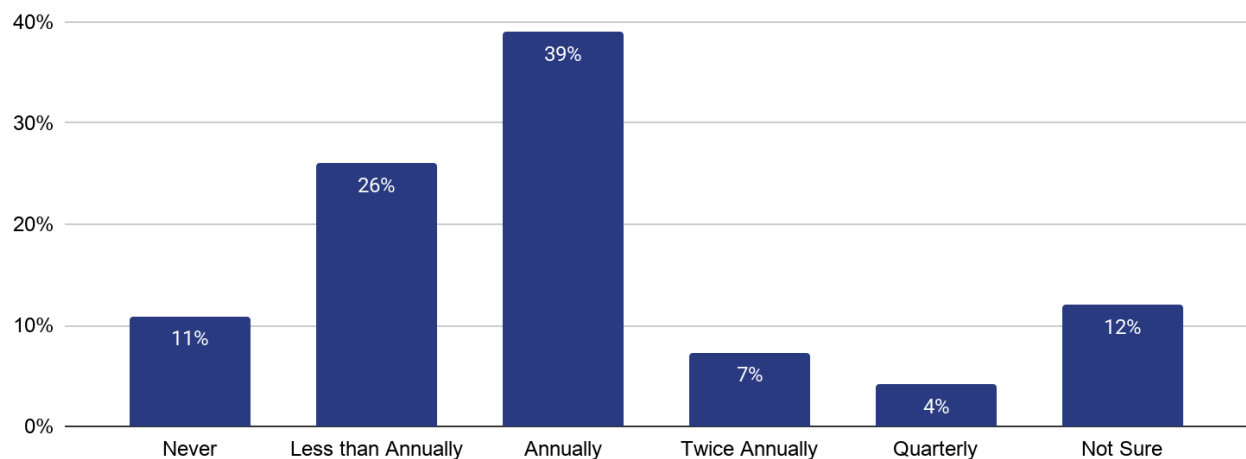
How prepared is your district to recover from a ransomware or cybersecurity incident?



Incident Response Plan Testing

When asked about incident response plan testing, the majority of respondents reported testing annually at most, with a combined 37% testing *less than annually* (26%) or *never* (11%). Only 11% test *quarterly* or *twice annually*, and 12% were *not sure*. **Compared to responses above, confidence in recovery readiness may be outpacing the practice that would validate it.**

How often does your district test its cybersecurity incident response plans?



AI Landscape

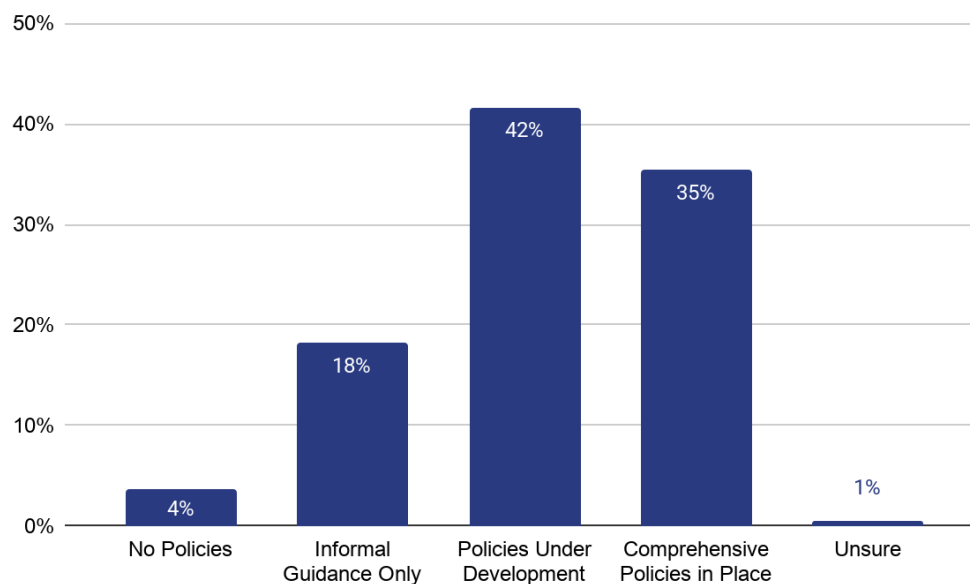
To understand the rapidly changing AI landscape, the survey posed several questions. An interesting theme emerged in that **AI is viewed as both a concern to mitigate and a tool to address concerns.**

AI Governance

Formal AI policy work has progressed more than some of this report's other AI measures. More than three-quarters of districts have either comprehensive policies in place (35%) or policies under active development (42%). Only a small minority (4%) report having no policies at all, and just 1% were unsure. The remaining 18% rely on informal guidance but have not yet begun formalizing their AI governance.

When comparing this data to earlier legal and compliance findings, where the share of districts *not addressing AI legal risk at all* fell from 21% to 5%, a broader picture has emerged: **legal and policy infrastructure for AI moved further and faster this year than the other AI readiness dimension in this report.**

How has your district established formal policies governing AI use?

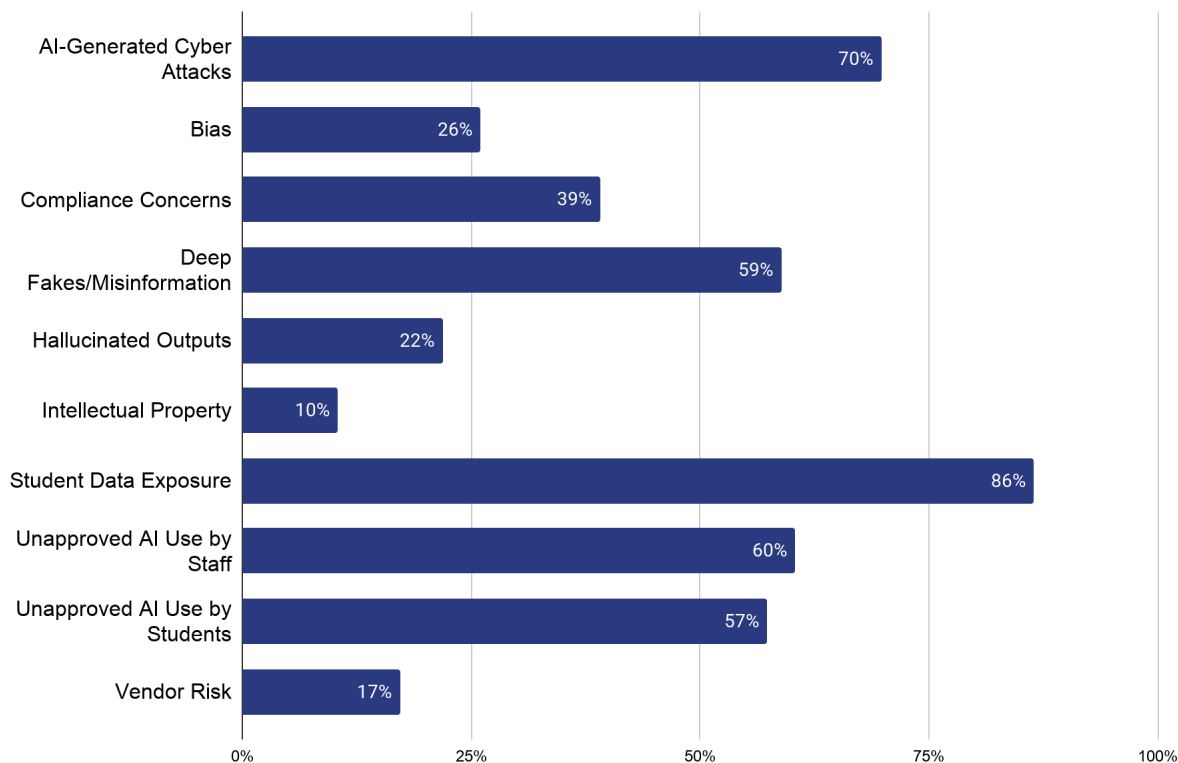


AI Risk

From a list of 10 items, respondents selected up to five AI-related risks that pose a concern. Student data exposure led by a wide margin, cited by 87% of respondents. AI-generated

cyberattacks followed at 70%. Notably, the next two highest-ranked risks involved internal use rather than external threats: unapproved AI use by staff (60%) and unapproved AI use by students (57%), alongside deepfakes and misinformation (59%). **Together, these responses suggest districts are at least as concerned about ungoverned AI use inside their own walls as they are about AI-enabled attacks from outside.** Concerns further down the list include bias (26%), hallucinated outputs (22%), vendor risk (17%), and intellectual property (10%), suggesting that these remain secondary concerns.

Which AI-related risks concern your district most?



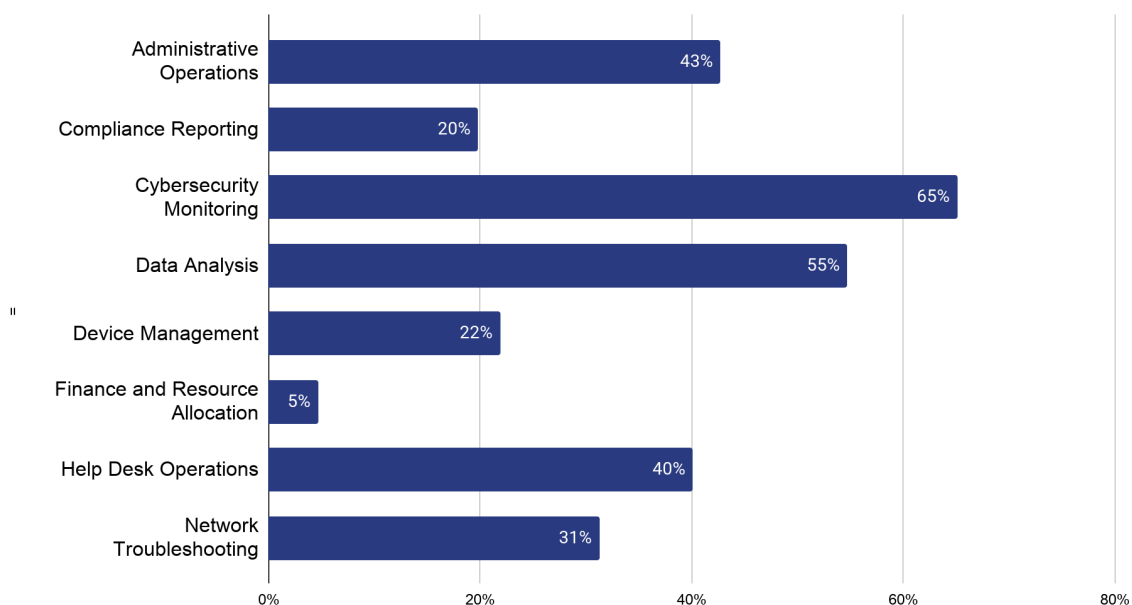
AI and Operational Value

Asked where AI and automation could provide the greatest operational value, the respondents pointed most often to cybersecurity monitoring (65%), followed by data analysis (55%) and administrative operations (43%). Help desk operations (40%) and network troubleshooting (31%) also emerged as having value. Finance and resource allocation drew the least interest at just 5%.

The prominence of cybersecurity monitoring here echoes the AI risk data above. Respondents indicated that they see AI as both a source of new cybersecurity exposure

and, at the same time, one of the areas where AI could most help address their cybersecurity concerns.

Where could AI and automation provide the greatest operational value?



Barriers to Progress

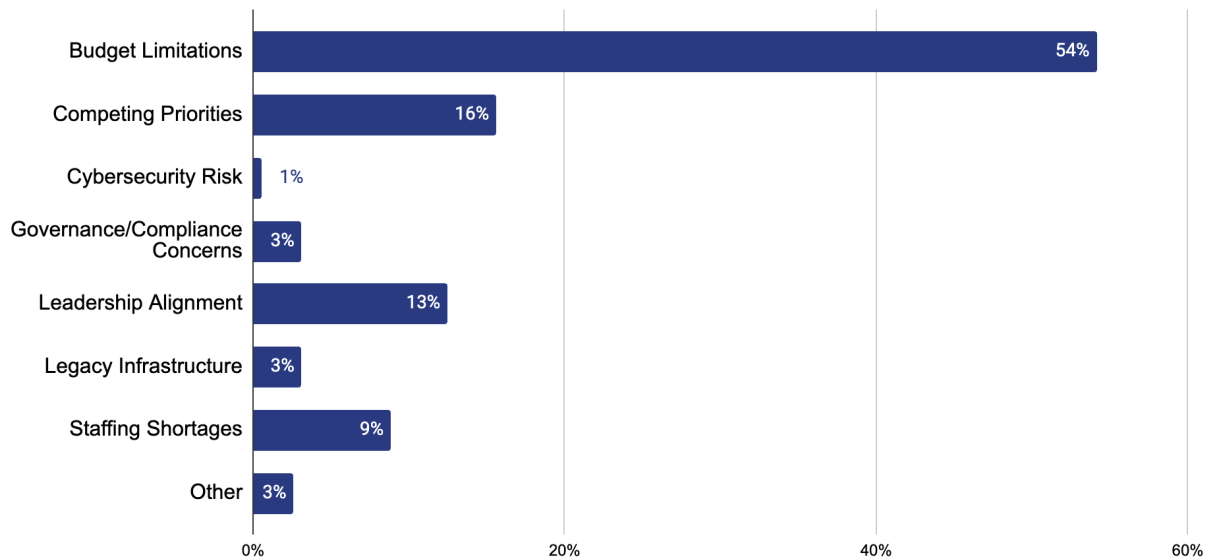
The final section of the survey asked respondents to reflect on their perceived barriers and challenges to making progress. As will be discussed, budget limitations emerged as one of the biggest challenges to address.

Budget Limitations

Asked to name the single biggest barrier preventing their district from advancing technology modernization efforts, 54% chose budget limitations. That is more than three times the share of the next-highest option, competing priorities (16%). Leadership alignment (13%) and staffing shortages (9%) followed, with governance/compliance concerns, legacy infrastructure, and cybersecurity risk each selected by 3% or less.

Budget concerns presented a consistent pattern throughout this report. Budget constraints emerged as one of the top cybersecurity challenges, and several respondents to this specific question about barriers named budget or funding directly in the “other” category.

What is the single biggest barrier preventing your district from advancing technology modernization efforts?

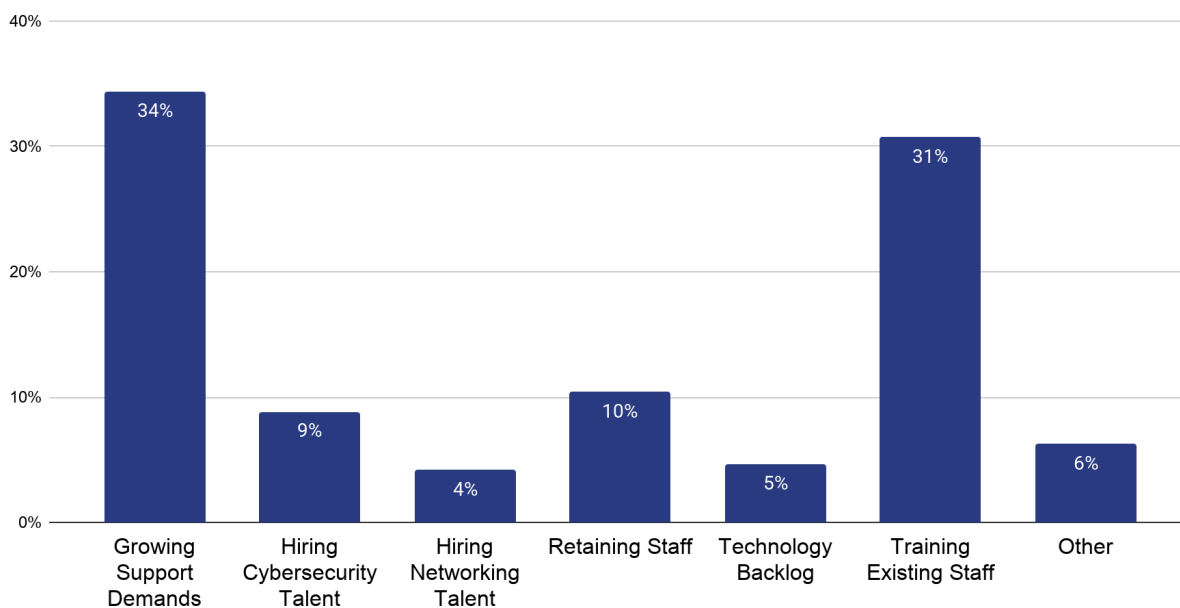


Staffing Challenge

Asked which single staffing-related challenge most impacts their district's technology strategy, respondents pointed overwhelmingly to capacity versus hiring. Growing support demands (34%) and training existing staff (31%) together account for nearly two-thirds of responses, while both hiring-related options (hiring cybersecurity talent and hiring networking talent) account for just 13%. Retaining staff sits at 10%.

The 12 respondents who selected "Other" rather than one of the six listed staffing challenges wrote in free-text responses. **Budget and funding emerged as the predominant theme.** The remaining open-responses referred to staff capacity and headcount.

Which staffing-related challenge most impacts your district's technology strategy?



Key Takeaways

Districts made progress on AI and cybersecurity readiness this past year. Among what can be compared with the 2025 results, legal and compliance readiness saw the sharpest improvement, while leadership remained nearly unchanged. Respondents indicated that their districts demonstrated improvement for understanding and managing AI risks, though many are still defining where AI aligns with their broader strategy.

Cybersecurity emerged as the clearest area of agreement among respondents as 58% of districts ranked it as their top technology priority and 84% placed it in their top three. At the same time districts see enormous potential for AI to improve cybersecurity operations with 65% identifying AI as the area with the greatest potential operational value in cybersecurity monitoring. At the same time, districts are grappling with the risks created by AI itself. That creates a familiar challenge for district leaders – how to unlock the benefits of a technology while putting guardrails around the risks.

Finally, funding emerged as a clear thread throughout the survey. Budget limitations were named the single biggest obstacle to technology modernization by over 50% of respondents, and budget concerns appeared in questions where “funding” was not a provided answer choice. **Across technology, staffing, cybersecurity and AI, districts are being asked to do more but without the resources to sustain the work. Until the K-12**

funding gap is addressed, it will remain challenging for districts to translate readiness into long-term capacity.

About CoSN



CoSN, the world-class professional association for K-12 EdTech leaders, is driven by a mission to equip current and aspiring K-12 education technology leaders, their teams, and school districts with the community, knowledge, and professional development they need to cultivate engaging

learning environments. Visit cosn.org or email membership@cosn.org to find out more about CoSN's focus areas, annual conference and events, advocacy and policy, membership, and the CETL® certification exam.

About HPE



HPE is a leader in essential enterprise technology, bringing together the power of AI, cloud and networking to help organizations achieve more. As pioneers of possibility, our

innovation and expertise advance the way people live and work. We empower our customers across industries to optimize operational performance, transform data into foresight, and maximize their impact. Unlock your boldest ambitions, with HPE. Discover more at [HPE.com](https://hpe.com).

About FullScale



FullScale is a national K-12 education nonprofit driving coherent K-12 systems transformation in practice, policy, people, and progress to create more personalized, competency-based and whole-child learning experiences for every student. Visit www.fullscalelearning.org to find out more.