Cybersecure 2025 Report

SECURE LEARNING FOR EVERY DIGITAL IDENTITY

Introduction

The wealth of sensitive data in school systems across the country has long made them attractive targets for cybercriminals. In fact, the education sector's reported cyber risk recently went from "moderate" to "high," with incident costs more than tripling in just the past year. This growing threat is particularly acute when it comes to student data – as learning becomes increasingly digital, protecting student identities has emerged as the new frontier in education cybersecurity.

The stakes are significant: according to the U.S. Department of Education, a single stolen student record can go for up to $300 on the dark web – significantly more valuable than most other types of personal data. Today's students leave digital footprints that encompass everything from personal data and academic records to behavioral patterns and learning preferences. While schools often have robust security measures in place for staff and administrative accounts, student accounts typically have fewer protections, making them an increasingly appealing target for cybercriminals. Even more concerning, the impact extends beyond immediate security breaches – compromised student identities can lead to long-term consequences as stolen personal information can remain vulnerable for years before the theft is discovered, potentially affecting students' future financial, educational, and employment opportunities.

What is a Digital Identity?

In K-12 education, a digital identity is the collection of online credentials and data that represent an individual within a school system. For students, this may include their login accounts and passwords, personal information (name, age, contact details), academic records and app access permissions. Digital identities are critical to support learning but if compromised, they can unlock access to sensitive information.

Our annual survey findings paint a sobering backdrop: 74% of administrators believe a security incident is likely to impact their school system in the coming year, up from 71% last year. The number of surveyed administrators reporting cyber attacks has also increased from 31% to 36%. Among school systems reporting incidents, phishing attacks remain the predominant threat – accounting for 87% of incidents, up from 73% last year. We also observed a notable shift in administrators' threat perceptions: 50% of 2024 survey respondents view ransomware as a likely threat, compared to 34% in 2023.

This year's report examines how school systems are adapting their security strategies to protect their most vulnerable users while navigating new challenges from AI adoption, mobile device policies, and increasingly complex edtech ecosystems. Through insights gathered from over 500 administrators nationwide, we explore the critical steps schools must take to safeguard student data and digital identities in an increasingly hostile cyber landscape.

Rising Cybersecurity Concerns in Schools

74% of administrators believe a security incident will impact their school system this year, up from 71% last year.

Dig deeper: The types of cyber attacks school systems face seem to vary by size. Larger ones (25,000-49,999 students) that experienced attacks reported dealing with a wider variety of threats – 60% reported ransomware, 80% reported DDoS attacks, and 80% dealt with student-on-student hacks, rates significantly higher than smaller school systems where these incidents were less common.

Clever

Key Findings

5%

READ MORE

of students have multi-factor authentication protection; **90%** teachers; **95%** IT staff

70%

READ MORE

of administrators believe AI is increasing **cybersecurity** risks.

1 in 4

school systems report increased cyberattacks

specifically targeting student accounts.

READ MORE

46%

READ MORE

of school systems are considering or implementing **zero trust** approaches.

45%

READ MORE

of school systems are using or considering fully **cloud-based** identity solutions.

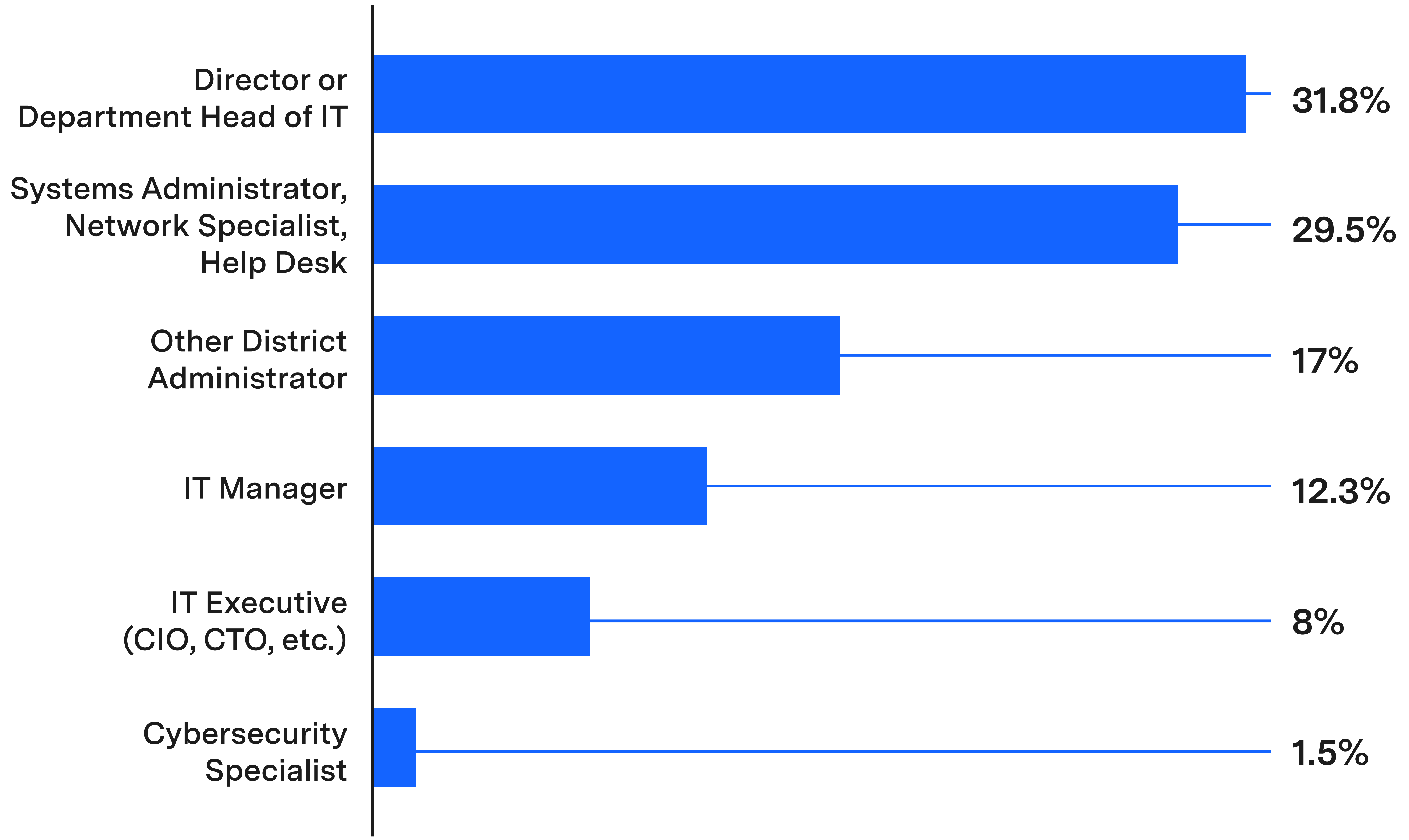
> “When I presented the statistics on daily attacks to district leaders, eyes went wide—people didn’t realize the **scale** of what we face every day.”

NEAL KELLOGG | DIRECTOR OF DIGITAL PROCUREMENT AND DATA PRIVACY | OKLAHOMA CITY PUBLIC SCHOOLS

Methodology

In Q4 2024, Clever conducted an annual survey of over 500 US-based administrators to develop a comprehensive perspective on the state of K-12 cybersecurity. The survey pool comprised administrators from Clever's user base nationwide. About 52% of administrators surveyed had roles directly related to information technology, including job titles such as Director of IT, Chief Information Officer, Chief Technology Officer, or IT Manager; another 30% were Systems Administrators or Network Specialists.

Which of the following is closest to your role or area of work?



Acknowledgements

We collaborated with administrators and field leaders to develop this report, incorporating their qualitative insights that influenced our key findings. We would like to express our gratitude to these forward-thinking Clever partners:

Corey Lee
Security CTO, Microsoft Education

Julia Fallon
Executive Director, SETDA

Neelam Ashok
Director, AISL Harrow Schools

Aaron Smith
CTO, Loudoun County Public Schools

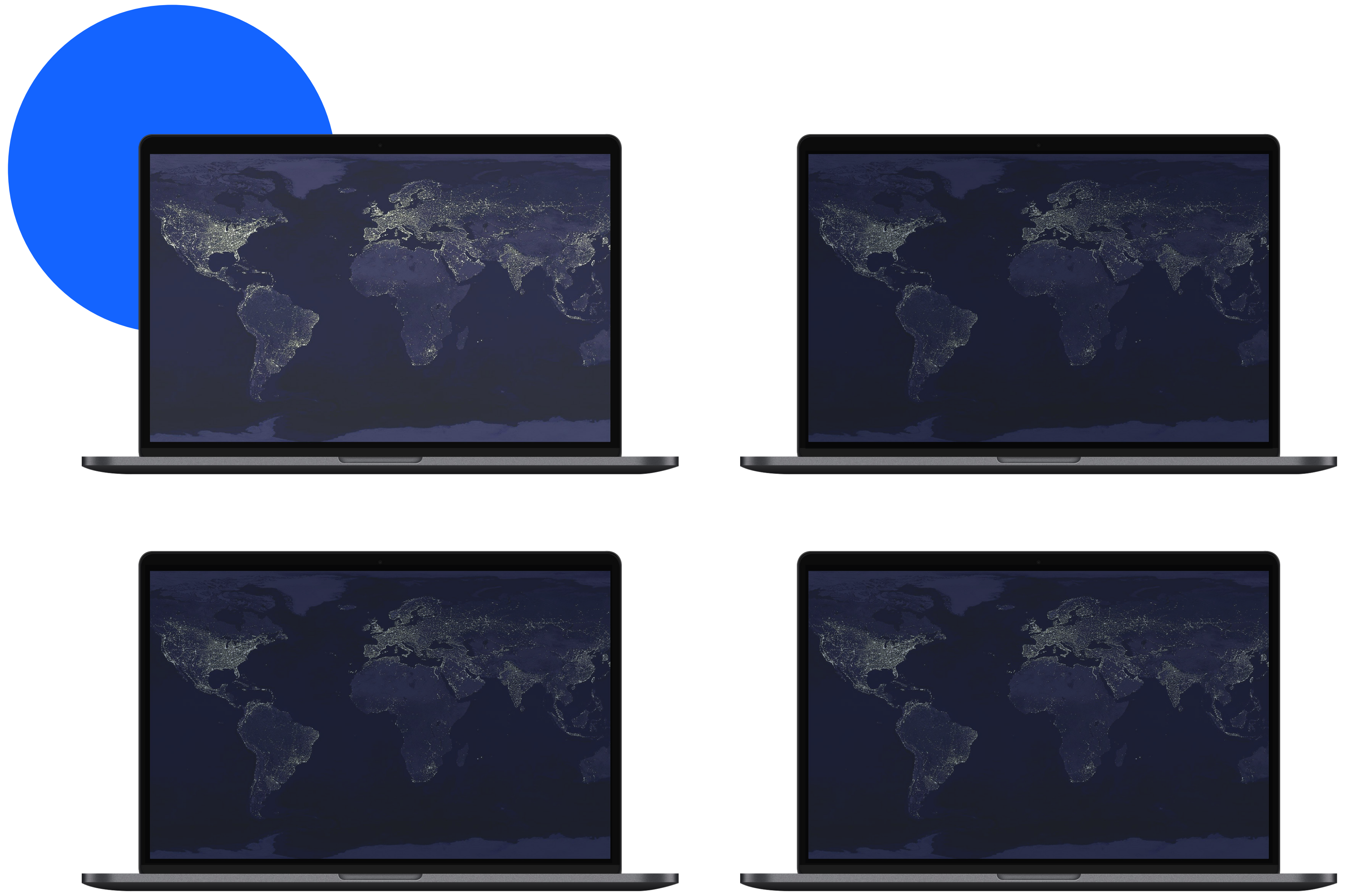
Kristin Bowling
Director of Technology Services,
Enterprise Elementary School District

Neal Kellogg
Digital Procurement and Data Privacy,
Oklahoma City Public Schools

Student Digital Identity: The New Security Frontier

The vulnerability of student digital identities represents a growing security crisis in K-12 education. While one in four school systems (25%) report increased cyberattacks specifically targeting student accounts, these remain the least protected digital identities. The disparity is striking – 95% of IT staff and 90% of teachers are protected by multi-factor authentication, while only 5% of students have similar safeguards.

While **1 in 4 districts** report increased cyberattacks specifically targeting student accounts,



only **5%** of students have multi-factor authentication protection

compared to

90% of teachers

95% of IT staff

“Whether you’re LA Unified or a smaller school system like ours, deploying student multi-factor authentication (MFA) presents **significant challenges.** Factors like limited device availability, the inability to provide YubiKeys to all students, and upcoming cell phone regulations for 2026 make it difficult to balance security, accessibility, and school system policies effectively.”

KRISTIN BOWLING | DIRECTOR OF TECHNOLOGY SERVICES |
ENTERPRISE ELEMENTARY SCHOOL DISTRICT

The Multi-Layered Challenge of Student Protection

The challenges in protecting student accounts are multifaceted and complex. **Nearly half of administrators report struggles with protecting students from online threats (45%) and maintaining student data privacy (45%), while an overwhelming 61% cite broader cybersecurity concerns as their primary identity management challenge.** School systems must balance robust security measures with ensuring students can easily access the tools and resources they need to support their learning. This balancing act is further complicated by the unique characteristics of student users – from varying age groups and digital literacy levels to the sheer number of students requiring protection.

Confidence Gap in Identity Protection

Only 24% of administrators feel "very confident" in their ability to protect student digital identities, while confidence drops even lower for parent accounts at 12%. This crisis of confidence reflects broader challenges school systems face in securing their entire school community. **Despite rising threats, less than 10% of schools have adopted sophisticated security approaches like risk-based authentication or zero trust principles (17%) that could better safeguard personal data.** This gap is particularly concerning, given that cybercriminals increasingly target student accounts precisely because of their weaker security. These accounts often have extensive permissions across numerous learning applications, which bad actors can use to move laterally through school networks and potentially escalate their access to more sensitive systems.

Clever

Admin's confidence in their ability to protect digital identities:

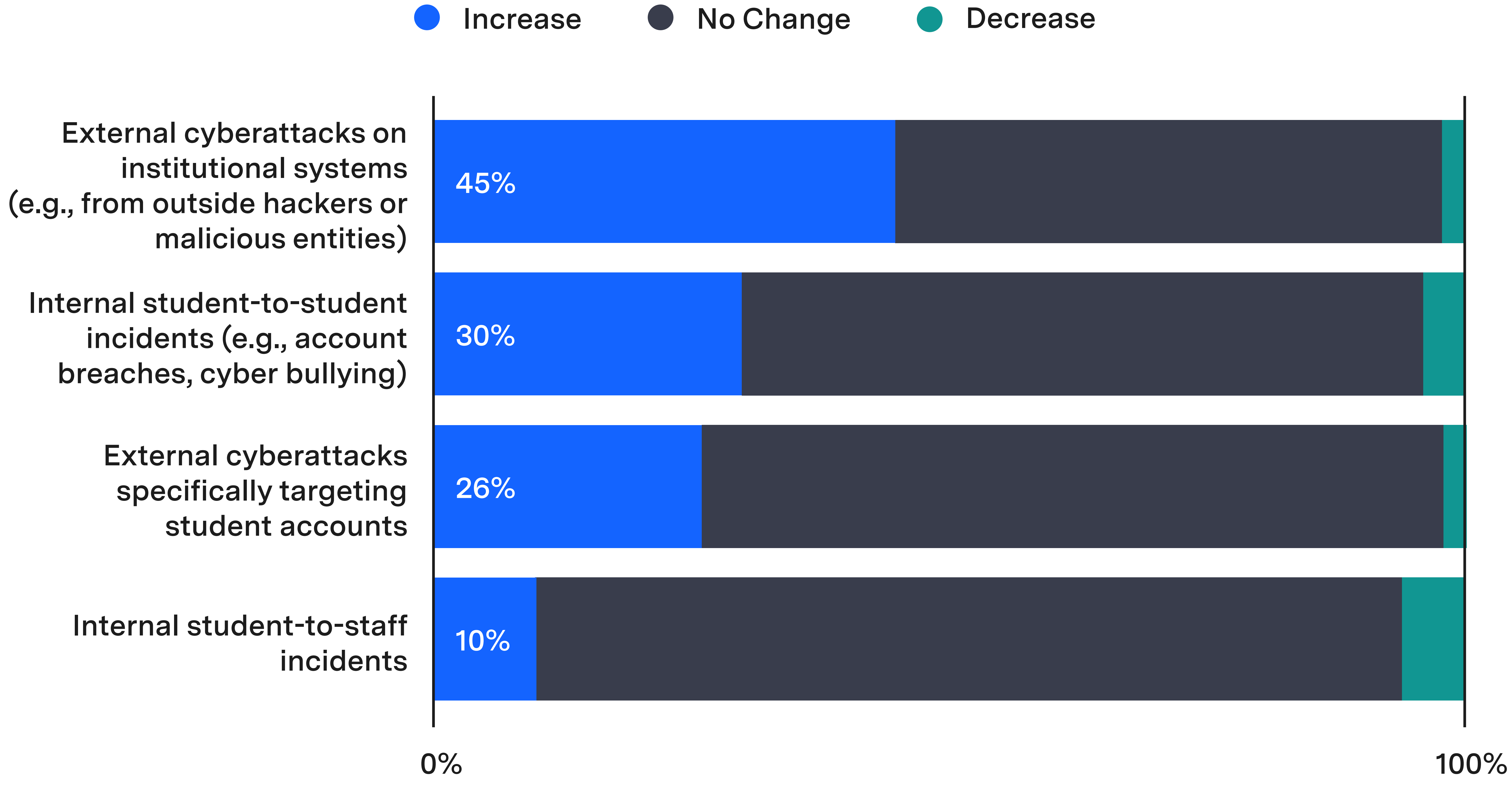
24% student accounts

12% parent accounts

Beyond External Threats: Schools Face Challenges from Within

Internal threats are growing alongside external ones – nearly one-third of schools (29%) report an increase in student-to-student security incidents, highlighting that cybersecurity challenges aren't just coming from outside the school walls. These internal incidents add another layer of complexity to school systems' security challenges, particularly as they try to balance student access with protection.

In the past year, have you observed changes in cybersecurity incidents targeting your institution?



Hot-Button Issues, Hidden Security Risks

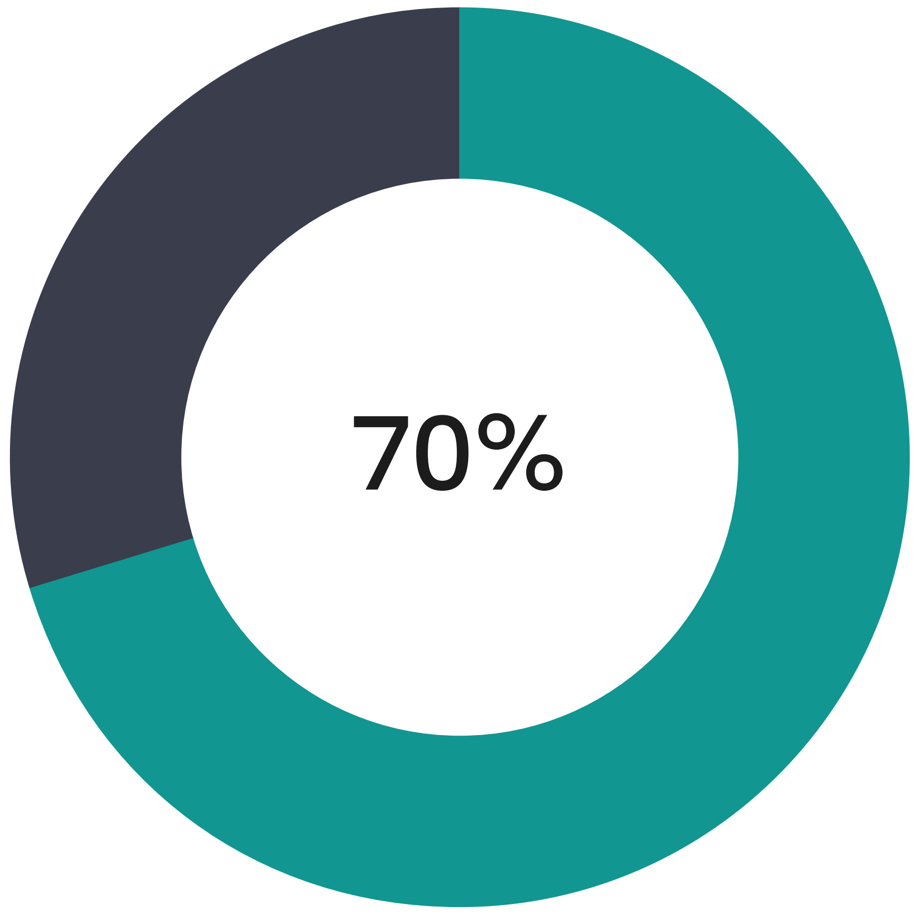
K-12 cybersecurity strategies do not exist in a vacuum. As schools navigate evolving educational trends and policies – from the rapid integration of AI to growing cell phone bans – these shifts create ripple effects across the security landscape. Today's technology leaders must balance traditional security concerns with new challenges stemming from broader educational policies, as solutions for one issue can often introduce unexpected security risks.

The AI Security Paradox

The rapid adoption of AI in education has created new security vulnerabilities that school systems are struggling to address. While 70% of administrators believe AI is increasing cybersecurity risks, schools lack preparedness to manage this threat. Only 46% have any process for vetting AI in edtech products, and a mere 9% have formal procedures – highlighting a critical gap between recognized risk and practical oversight.

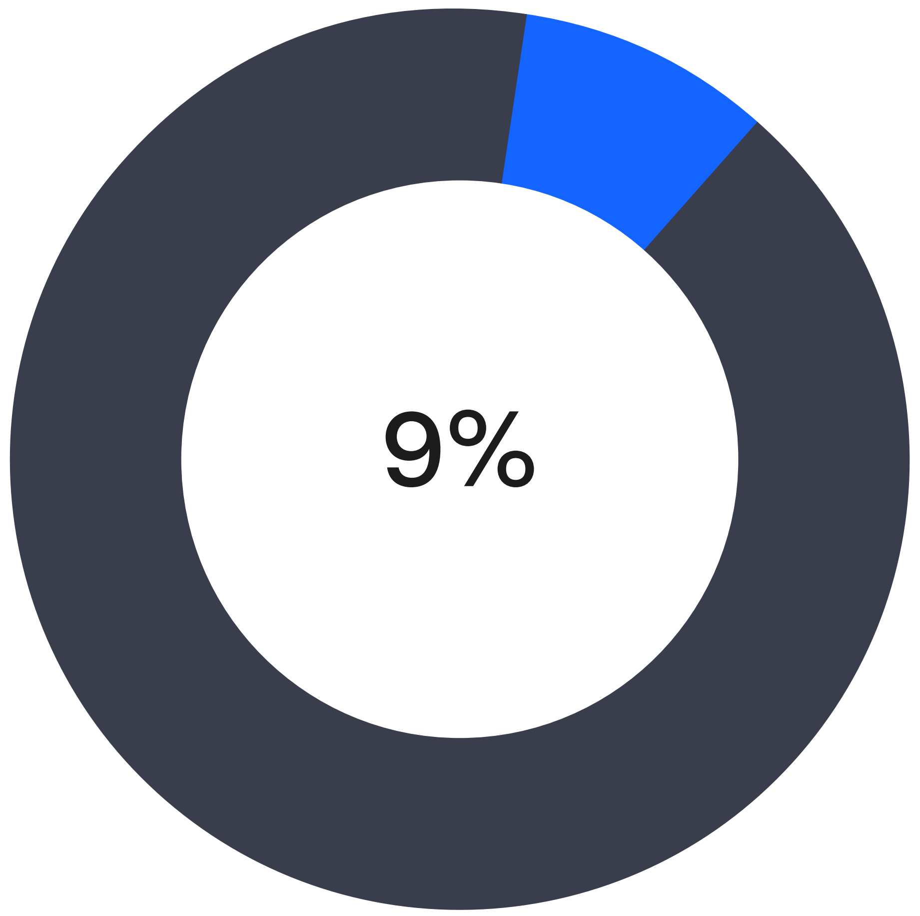
The AI Security Paradox in Schools

Despite widespread concern about AI security risks, few schools have formal safeguards in place



Perceive Increased Risk

7 in 10 schools report AI is increasing their cybersecurity risks



Have Formal Vetting

Only 9% have established formal processes to evaluate AI in edtech

"The growing adoption of AI in K-12 schools brings exciting opportunities for teaching and learning, but also introduces **new considerations** for district technology leaders. Districts need clear ways to evaluate these tools across multiple dimensions – from data privacy and security to evidence of effectiveness and equity – to ensure AI-powered products can deliver on their innovative potential while **protecting** student identities."

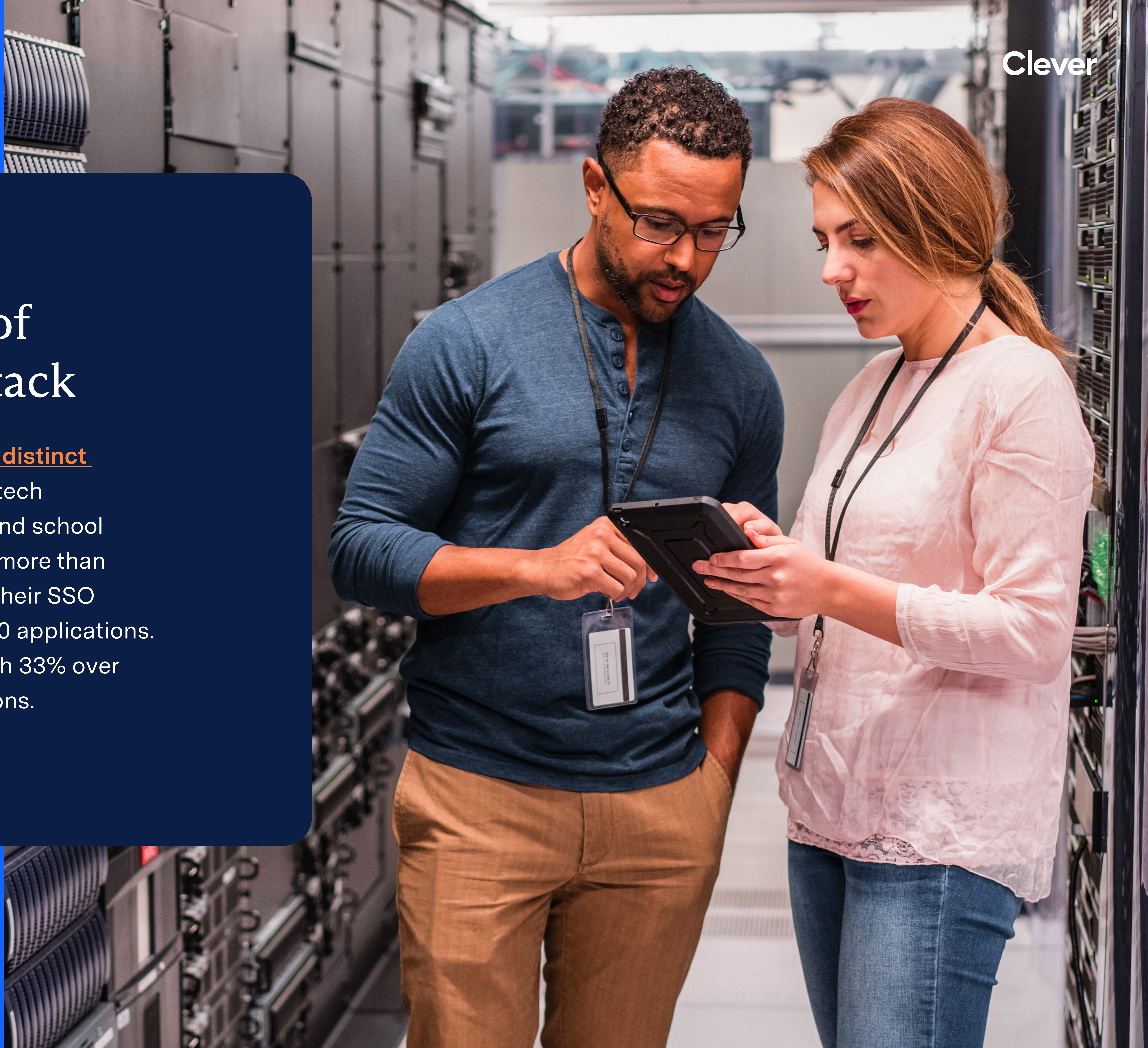
JULIA FALLON | EXECUTIVE DIRECTOR | SETDA

Cell Phone Policies Shape School System Cybersecurity Strategies

With 60% of school systems moving to restrict student phones and nearly half believing this will improve security, K-12 leaders face a clear imperative: developing authentication approaches that protect student accounts without depending on personal devices. This stands in contrast to staff security, where 75% of schools rely on personal mobile devices for authentication. As more school systems adopt these policies, this creates an immediate need for schools to develop new approaches to student authentication that align with both modern security needs and evolving classroom policies.

Future Trends: Evolution of the School System Tech Stack

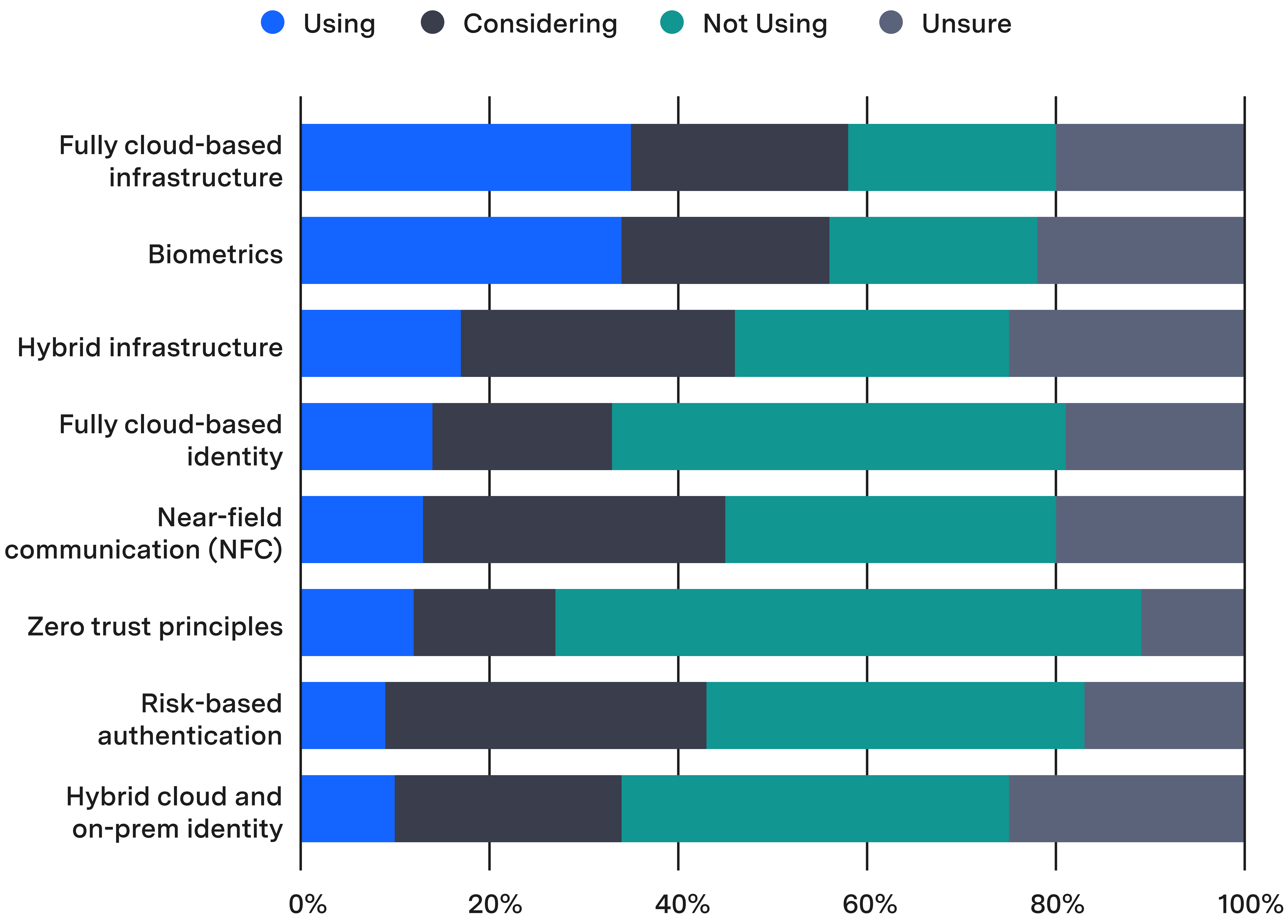
With school systems juggling an astounding 2,739 distinct edtech tools annually, the complexity of school edtech ecosystems has reached unprecedented levels – and school systems are struggling to keep pace. 18% manage more than 21 applications requiring individual logins outside their SSO platform, while another 32% manage between 6–20 applications. Larger school systems face greater complexity, with 33% over 25,000 students managing more than 30 applications.



The Shift Toward Modern Security Architecture

Zero trust adoption – an approach that requires all users to verify their identity every time they access resources, regardless of location or previous access – varies significantly across school systems, with 46% either using or considering zero trust principles. Larger school systems are leading this transformation: 66% of school systems with over 50,000 students are either considering or implementing zero trust approaches. Similarly, while 35% of school systems currently use hybrid cloud and on-premise identity solutions, only 13% have fully moved to cloud-based management, though another 32% are actively considering it. This slow adoption suggests school systems face obstacles beyond technical challenges, including budget constraints and training needs.

Is your district using or moving toward use of any of the following?



"Smaller school districts can adopt Zero Trust by focusing on IT architecture simplification and modern security operations to maximize existing resources. **Reducing complexity** in IT environments enables districts to better leverage current tools and talent, enhancing visibility and response to threats without overextending budgets or personnel."

COREY LEE | SECURITY CTO | MICROSOFT EDUCATION

Disconnected Tools Exacerbate Resource Constraints

Most school systems are managing security through multiple tools rather than a unified platform. **While 45% report using multiple specialized tools in a "layered approach," only 13% are actively working to consolidate these tools.** This fragmentation creates significant challenges – IT teams must maintain and monitor multiple systems while training staff on various platforms. The impact is evident, with 63% of districts citing limited cybersecurity awareness among non-IT staff as a top barrier. This challenge is amplified when staff must also learn and navigate different interfaces, authentication methods, and security protocols across disparate systems.

Dig deeper: School systems are gradually moving toward more sophisticated identity protection measures. Nearly a quarter are considering risk-based authentication (23%), while others are evaluating biometric security measures (15%). These explorations indicate a growing recognition that traditional security approaches may no longer be sufficient for today's threats, even as school systems struggle with implementation challenges.

Growing Cybersecurity Demands Outpace Resources

The gap between security needs and available resources continues to widen. More than half of school systems (53%) report insufficient cybersecurity spending, virtually unchanged from last year. More telling, satisfaction with current spending levels has dropped significantly – only 31% of administrators believe they're spending the right amount on cybersecurity, down from 41% in 2023.

Clever

Federal Funding Falls Short of School System Needs

School systems nationwide have overwhelmingly sought FCC E-rate funding for cybersecurity improvements, with requests far exceeding available resources. Nearly half (47%) applied for funding to implement advanced firewalls, identity and access management solutions, and other cybersecurity tools, and 83% of applicants expect these upgrades would significantly strengthen their security posture. However, the stark reality of demand versus funding has emerged – **while the FCC allocated $200 million for the program, they received $3.7 billion in requests from schools and libraries, representing demand that exceeded available funding by 1,850%.**

Dig deeper: This insight reflects recent findings from SETDA, the 2024 State Edtech Trends, which found state leaders' confidence in cybersecurity funding has plummeted. Those believing their state provides "sufficient" funding dropped from 19% to 8%, while those reporting only minimal funding more than doubled from 15% to 33%. This shift may reflect either actual funding decreases or a growing recognition that previous funding levels are inadequate to address escalating cyber threats.

E-Rate Program Funding Gap

Personnel Shortages Hinder Security Progress

Despite strong organizational alignment on cybersecurity priorities – with leadership support and staff buy-in ranking as the least challenging issues (34% and 36% respectively) – school systems face significant operational hurdles. Staffing shortages remain the biggest challenge, with the percentage of administrators ranking it as their top concern increasing from 32% to 37% year over year. This personnel crisis is compounded by broader implementation challenges – **63% cite limited cybersecurity awareness among non-IT staff as a top barrier to improvement.** Meanwhile, budget constraints remain the second most pressing issue, with 23% of administrators rating it their top challenge.

Conclusion

Secure Digital Identities in 2025 with Confidence

Cybersecurity in K-12 education is more critical than ever as schools embrace digital transformation. With increasing cyber threats, protecting student and staff identities shouldn't add to your stress. Discover practical steps to safeguard your district in Clever's Cybersecure 2025 Action Plan.

Key Recommendations at a Glance

- **Prioritize student account protection:** Students are prime targets for cyberattacks. Strengthen your district's defenses with robust student account security measures.
- **Modernize identity and access management:** Implement a zero-trust security model supported by automated identity and access management tools.
- **Choose classroom-friendly solutions:** Enhance classroom safety with innovative security solutions that reduce reliance on devices for multi-factor authentication (MFA).
- **Build a collaborative security ecosystem:** Partner with vendors, state agencies, and the edtech community to create a transparent, effective cybersecurity ecosystem.

Ready to Act?

Access Clever's 2025 Action Plan for step-by-step guidance to secure your district's digital future. Whether you're taking the first step or optimizing your current strategy, our actionable insights will help you protect digital learning—and find some peace of mind along the way.

Explore the Action Plan Now

Clever

Clever is on a mission to connect every student to a world of learning. More than 77% of U.S. K-12 schools use Clever to power secure digital learning experiences. With Clever's layered security solutions, K-12 schools can protect district access and identities for all staff, teachers, and students. With a secure platform for schools and a network of leading application providers, Clever is committed to advancing education with technology that works for students everywhere. Clever, a Kahoot! company, has an office in San Francisco, CA, but you can visit us at clever.com anytime.

W/A Whiteboard Advisors

Whiteboard Advisors is a mission-driven communications, research, and consulting firm that supports organizations working to advance educational equity and economic mobility. Our clients include the nation's most respected philanthropies, companies, nonprofit organizations, and investors. Our work is truly multidisciplinary, sitting at the intersection of business, policy, practice, and the media.

Clever