Clever

Cybersecure 2025 Report

SECURE LEARNING FOR EVERY DIGITAL IDENTITY

Executive Summary

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.

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.

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.

Executive Summary

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.

01. Students' Digital Identities Emerge as Prime Cyber Target: While external attacks on school systems continue to rise, student accounts have become the new frontier of cyber risk with only about 5% of students protected by MFA compared to 90% of staff.

02. Most School Systems Lack Confidence in Protecting Student Digital Accounts: Only 24% of administrators express high confidence in their ability to protect student identities, with even lower confidence (12%) in parent account security.

03. Internal Security Threats Rise Alongside External Attacks: The threat landscape has expanded beyond external actors, with 29% of school systems reporting increases in student-to-student security incidents, creating a dual challenge of protecting against both external and internal risks.

04. AI Security Risks Are Outpacing School System Safeguards: 70% of administrators identify AI as a growing security concern, yet only 9% have formal vetting procedures for AI in edtech products, highlighting a critical gap between risk awareness and readiness.

05. Amidst Cell Phone Bans, Student Security Requires Different Solutions: 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.

Expert voices

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.

On cyber attacks:
"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*

On AI:
"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*

On cell phone bans:
"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 Enterprise Elementary School District in CA*

On the future:
"AI gives me immense hope for the future of cybersecurity. By accelerating zero-trust adoption and automating security operations, AI has the potential to transform how we defend underserved environments and empower individuals to join the fight. It's about leveraging innovative technology alongside humans to advance K-12 cyber defense." - *Corey Lee, Security CTO, Microsoft for Education*

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.

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.