Clever

Cybersecure 2026 Report

CLOSING THE IDENTITY GAP FOR GLOBAL EDUCATION

Foreword

By Corey Lee, Security Chief Technology Officer, U.S. SLED at Microsoft

To weather scientists, a "perfect storm" is an exceptionally rare, catastrophic event created by the convergence of multiple, independent weather systems that amplify each other's intensity. In my daily role as Security Chief Technology Officer for U.S. SLED at Microsoft, I see AI-powered technologies and existing security systems increasingly colliding with bad actors willing to exploit their flaws. I feel like a meteorologist who can tell that those weather systems are dangerously close to one another, inching towards landfall every day. The threat landscape is changing, and security architecture, identity, and emerging technologies like AI will have to change with it – or else catastrophic consequences may ensue.

From that perspective, one thing is clear: cybersecurity in education has entered a new phase.

The data in this report **mirrors what Microsoft sees globally.** Education institutions are now among the most frequently targeted sectors, with disproportionate levels of identity and business email compromise compared to other industries. This is not incidental. Schools are uniquely open, complex, and resource-constrained, and adversaries have learned to exploit that reality. Increasingly, threat actors do not just attack education for disruption or ransom; they incubate there, harnessing the information gleaned from compromised identities, accounts, and trust relationships to hack into other parts of critical infrastructure while impacting the lives of students, teachers, and parents. That makes K-12 cybersecurity not only an institutional concern, but a broader community and national security issue.

At the same time, artificial intelligence has moved from the realm of experimentation to day-to-day use, evolving faster than the underlying systems that were designed to support it. IT leaders and staff, too, have struggled to keep up with rapidly changing AI technologies and the accompanying threat landscape. This gap between the reality of AI's security impact and schools' capacity to handle it has reshaped how education leaders think about risk, trust, and readiness.

AI isn't just creating entirely new cybersecurity problems; it's amplifying unresolved ones. AI systems are layered on top of preexisting identity frameworks, data environments, applications, and infrastructure. When those foundations are immature, AI makes the gaps more visible.

This is why conversations about AI in education turn into conversations about identity and data. Identity has become a Zero Trust control plane for modern environments, and students, staff, vendors, parents, and partners interact across thousands of applications and devices. As a result, education is one of the most identity-dense sectors in the economy. This data is the currency that powers AI, yet many schools are still working to fully understand what data they have, where it lives, and how it is governed. AI alone doesn't increase risk, but when AI-enabled tools are introduced into environments lacking strong identity governance or data controls, risk increases because those underlying systems were never fully secured to begin with.

Schools and districts receive little external support to navigate these challenges, as funding sources have shifted and federal and state leaders have only slowly released standards and policies offering real-world guidance. Consequently, in the absence of government leadership, cybersecurity insurance providers have played an outsized role in driving behaviors. As insurers raise expectations around controls like multi-factor authentication, endpoint detection, and incident readiness, the baseline for "acceptable" security hygiene is changing. In many cases, this is driving long-overdue progress toward fundamentals. In others,

it exposes the strain placed on small teams who are being asked to meet enterprise-grade standards with limited resources. From where I sit, the question is not whether these controls are necessary (they are) but how the ecosystem supports districts in meeting them before an incident, not after one.

This report, much like **Microsoft's own recent report,** does not prescribe a single path forward, but it does surface the patterns that matter most right now: the urgency of securing identities at scale, the need to treat AI as part of a broader system rather than a standalone tool, and the importance of shared responsibility across districts, vendors, insurers, and policymakers.

As we venture into this perfect storm, my hope is that education leaders will move beyond reactive security conversations and toward intentional design. Because in this next chapter, the ability to innovate safely will depend less on any single technology, and more on the strength of the identity and trust systems beneath it.

Corey Lee

Security Chief Technology Officer

U.S. SLED at Microsoft

Executive Summary

One in Two U.S. School Districts Have Experienced a Cybersecurity Incident

In 2025, 52% of U.S. districts experienced a cybersecurity incident, up from 36% in 2024 and 31% in 2023. Moreover, districts that experienced a breach are more likely to believe another attack is likely, underscoring how deeply incidents shift perceptions of risk. Leaders in the UK, Canada, and Australia describe a similar pattern, where experiencing an incident fundamentally changes how school systems assess their own vulnerability.

Third-Party Incidents Highlight the Reality of Shared Risk

Vendor-related incidents in U.S. districts rose sharply from 4% in 2023 to 32% in 2025, reflecting the growing concentration of data and workflows in shared platforms. Leaders in the UK, Canada, and Australia describe the same dynamic: as schools rely on a small number of widely used systems, a single failure can create system-wide exposure.

Student Identity a Top Concern for U.S. Districts Despite Weakest Guards

Student identity theft or long-term harm is now the #1 concern for 54% of U.S. districts–yet only 21% of them feel most confident addressing student identity threats, and students remain the group with the lowest MFA adoption (12-15% across grade levels).

Cyberinsurance Mandates Are Rising – and Districts Need Simpler Paths to Compliance

More than half of U.S. districts (58%) have adopted new technologies to meet insurance requirements but only 12% believe these requirements have "significantly improved" their security, and nearly 40% are unsure whether the changes have helped at all, reflecting the reality that cybersecurity insurance decisions and day-to-day security operations are often owned by different parts of the organization.

AI is Amplifying Risk Faster than School Systems Can Respond

Four out of five U.S. districts believe AI is increasing their cybersecurity risk, yet only 11% have formal processes to vet AI use in edtech tools. Internationally, school system leaders echo this concern, describing AI-enabled phishing and impersonation attacks as more convincing, faster-moving, and harder for staff to detect.

Resource Constraints (Not Awareness) Are Now the Primary Barrier to Progress

Leadership support ranks as one of the least challenging issues for U.S. districts, but staffing and budget shortages continue to limit the ability to adopt, manage, and sustain modern security practices. Leaders in the UK, Canada, and Australia describe similar constraints, reinforcing that capacity, not intent, is the binding limitation across school systems.

Table of Contents

About the Authors

Evo Popoff is a senior vice president at Whiteboard Advisors. Named State Policy Maker of the Year by the State Education Technology Directors Association, he previously served as chief innovation and intervention officer and assistant commissioner for the New Jersey Department of Education, where he oversaw the state's edtech and school system improvement efforts. Prior to joining the department, he led the development of edtech products and school improvement solutions in collaboration with school system and state leaders and educators. Before beginning his career in education, Evo practiced law at McDermott, Will & Emery, where he worked on labor and employment, antitrust and general corporate issues. He holds a Bachelor of Arts in political science from the University of Chicago and a Juris Doctor from The George Washington University Law School.

Daimen Sagastume is a senior director at Whiteboard Advisors (W/A), where he specializes in advocacy and growth enablement across K-12 education. Prior to joining W/A, he spent five years at Emerson Collective, managing its education philanthropy investment portfolio with a focus on scaling innovative solutions for educational equity. During his tenure, he played a pivotal role in incubating Uppercase, a seed-stage edtech venture dedicated to democratizing access to world-class teaching expertise. A Stanford University graduate with a Bachelor of Science in biology, Daimen discovered his passion for education while pursuing premedical studies. At the intersection of edtech, philanthropy and strategic advisory, he works to ensure that innovative edtech solutions reach the students and educators who need them most.

Clever

Clever is on a mission to connect every student to a world of learning. As the leading identity platform for education, more than 111,000 schools worldwide use Clever to power secure digital learning experiences. With Clever's layered security solutions, schools can protect access and identities for all staff, teachers, and students. With a secure identity 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

For more than 20 years, Whiteboard Advisors has collaborated with the most transformative organizations, individuals and investors in education. Our diverse team of educators, wonks and storytellers brings in-depth understanding of policy, technology and practice to bear on cutting-edge research, powerful writing, and the design of communications and advocacy campaigns that challenge the status quo. Whether we're working with startups or the most established organizations in education, we're passionate about taking breakthrough ideas to scale.

Acknowledgments

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:

Adam Bird
Director of ICT, Hunter Valley Grammar School

Al Kingsley, MBE
Group CEO, NetSupport; Multi Academy Trust Chair, Department for Education UK; EdTech Advisor, NetSupport (UK based), plus governance roles in MATs

Andrea Bennett
Executive Director, CITE

Arman Jaffer
Founder & CEO, Brisk Teaching

Bruno Petitti
Executive Director of Digital Strategy, Ridley College

Chris Beddows
Headteacher / School Leader, Dwight School London

Chris Dale
Director of Security Services, Educational Collaborative Network Ontario

Corey Lee
Security CTO, Microsoft SLED

Cynthia Hays
Director of Risk Management, Oklahoma City Public Schools

Doug Levin
Director, K12 Security Information eXchange (K12 SIX)

James Clarke
Director of Digital Strategy in the UK

Eric Hileman
Executive Director, IT Services, Oklahoma City Public Schools

Gary Henderson
Director of IT, Millfield School, UK – Glastonbury, England

Julia Fallon
Executive Director, SETDA

Keith Krueger
CEO, CoSN

Mark Racine
Co-Founder, RootED Solutions

Matt Esterman
Founder, The Next Word

Matthew Given
CEO, Seesaw

Michael Klein
Senior Director for Preparedness and Response, Institute for Security + Technology

Nicol Turner Lee
Director, Center for Technology Innovation (CTI), Brookings Institution

Nicholas Little
Head of School, International School of Aberdeen

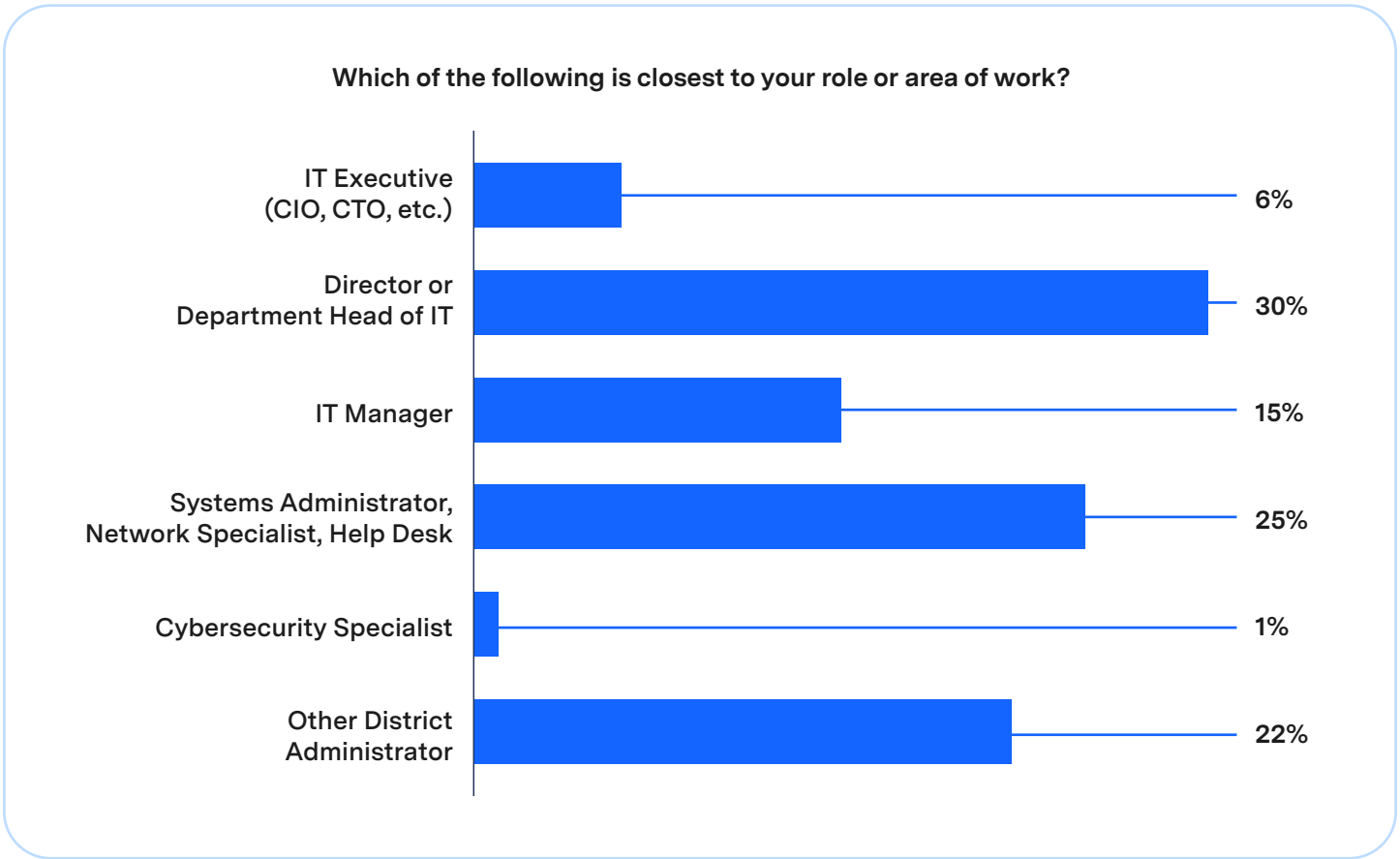
Sriram Seshadri
Head of Security, Clever

Stanley Nyanhi
IT Manager / IT Services Lead, Dwight School London

Methodology

In Q4 2025, Clever conducted its annual U.S. cybersecurity survey to understand how K-12 district leaders are experiencing, responding to, and preparing for evolving cyber threats. The survey gathered responses from over 500 administrators and technology professionals across districts of varying sizes, geographies, and demographics. As in prior years, the respondent pool primarily represented individuals in district roles with direct responsibility for technology and security decisions. Approximately 52% of respondents held titles such as Chief Technology Officer, Director of IT, or IT Manager. An additional 25% identified as Systems Administrators or Network Specialists. This methodology and findings presented in this section reflect U.S. districts only.

In addition to the U.S. survey findings presented in this report, Clever worked with ISC Research to conduct a separate qualitative and desk-based analysis to understand how school cybersecurity challenges are evolving internationally. This international analysis draws on curated interviews and publicly available guidance from the United Kingdom, Canada, and Australia. It is designed to provide comparative context, highlight shared pressures, and surface emerging risks and regulatory approaches.



Clever

UNITED STATES OVERVIEW

Cybersecure 2026 Report

CLOSING THE IDENTITY GAP FOR GLOBAL EDUCATION

Introduction

School districts today are navigating a cybersecurity landscape that is shifting faster than their systems, staffing, and budgets can keep pace. Cyberattacks are no longer episodic disruptions but persistent conditions under which schools now operate.

This year's Cybersecure Report examines how district leaders are responding to these realities – and where the sector still lacks the guardrails, capacity, and coherence needed to protect students and staff in an increasingly digital school environment.

Based on survey responses from K-12 technology and security leaders across the United States, the 2026 findings surface a clear narrative. Breaches have gone from "likely" to "probable," fundamentally reshaping district leaders' understanding of their own exposure. The report also includes an MFA Snapshot, highlighting that despite rising adoption, friction, workarounds, and mobile phone bans have complicated this foundational safeguard.

Cyber insurance has emerged as one of the most powerful – and most often misunderstood – drivers of security practice. Insurance requirements around MFA, identity management, and vendor vetting are reshaping district priorities, yet many leaders remain unsure whether these changes meaningfully improve their security posture.

Meanwhile, AI is accelerating threat activity and entering school environments faster than districts can evaluate or secure, creating a widening preparedness gap. And across all of these domains, resource constraints are now the most significant barrier to progress. Leaders know what strong cybersecurity requires, but staffing shortages, limited budgets, and tool complexity make it difficult to turn that knowledge into sustainable action.

Taken together, these findings illustrate a sector in transition: highly aware of its risks and increasingly aligned on priorities, but constrained by capacity and outdated infrastructure. The pages that follow explore each major theme in depth:

- K-12 Breaches Move from "Likely" to "Probable"
- The Identity Gap That Still Hasn't Closed
- MFA 2026 Snapshot: Progress Amid Persistent Challenges
- Cyber Insurance: Driving Practice but Delivering Mixed Results
- AI and Future Threats: An Unprepared Sector
- Resource Constraints: Awareness Without Capacity

This report aims to give education leaders, policymakers, and edtech partners a clearer picture of where the system stands today, and what it will take to build a more resilient, identity-centered security foundation for the years ahead.

Clever

K-12 Breaches Move from "Likely" to "Probable"

The cybersecurity pressure surrounding K-12 schools has intensified noticeably over the past two years. Last year, many district technology leaders expected a security incident. This year, a staggering one in two have lived through one. The baseline has shifted: cyber incidents are no longer hypothetical events districts plan around, but lived experiences shaping how they think about risk, resilience, and day-to-day operations. As Eric Hileman, Executive Director, IT Services, of Oklahoma City Public Schools, explains: "There's a growing acceptance in K-12 that cybersecurity incidents are, unfortunately, part of the landscape now. What's different in education is that when something happens, districts tend to help each other instead of going silent. That collaboration is baked into the culture."

One in Two Districts Now Breached

In many ways, breach prevalence has reached critical levels. In the past year, 52% of districts experienced a cybersecurity incident, a sharp increase from 36% in 2024 and 31% in 2023. That 21-percentage point rise in just two years underscores how quickly cyber threats are accelerating, often faster than districts' capacity to defend against them.

Not surprisingly, experiencing an incident changes how leaders see their own vulnerability. Among districts that have been breached, 80% believe another attack is "very likely" or "somewhat likely," compared to 64% of non-breached districts. According to Doug Levin, Director of K12 SIX, "If a school system has been a victim themselves, or even if a near neighbor has had an issue, they tend to take cybersecurity more seriously, at least for a period of time." But regardless of whether a breach has been suffered or not, for the majority of districts surveyed, they are a major concern.

52%

of districts experienced a cybersecurity incident, a sharp increase from 36% in 2024 and 31% in 2023

Phishing Remains the Dominant Attack Vector

At the same time, the nature of attacks is evolving. Phishing, which uses social engineering in the form of deceptive calls, texts, or emails to get people to reveal sensitive personal information, remains the dominant threat, accounting for 74% of reported incidents. Michael Klein, Senior Director for Preparedness and Response at the Institute for Security and Technology, says, “Any company and subprocessors that touch student or educator data should be using phishing-resistant multi-factor authentication. That should be table stakes. This kind of accountability needs to apply across the entire ecosystem, including vendors themselves.”

Ransomware Adds Financial Pressure to Data Risk

Meanwhile, ransomware attacks continue their steady climb, now representing 15% of reported incidents, adding direct financial and operational pressure on top of data exposure concerns. According to a recent global survey of 1,500 IT professionals in different industries, 61% of those in education had faced a ransomware threat between August 2024 and August 2025.

Vendor Breaches Surge

But the pattern of where and how schools are compromised is changing in important ways. Vendor data breaches have skyrocketed from 4% in 2023 to 32% in 2025, an almost eightfold increase. According to Eric Hileman, “Most of the incidents we’re dealing with now aren’t coming from inside the district. They’re coming through vendors.” Much of this reflects the ripple effects of major third-party incidents, such as the 2024 PowerSchool breach, and the central role shared platforms now play in school operations. Keith Krueger, CEO of CoSN, says, “Vendor data breaches are absolutely front and center after what happened with PowerSchool. But districts can’t just blame the vendor alone. They also have a responsibility to strengthen their own practices.” In other words, vendor responsibility is part of the story, but not the end of it. Arman Jaffer, Founder and CEO of Brisk Teaching, explains: “I think about cybersecurity as overlapping responsibility. District IT teams are doing incredible work, often with impossible constraints, but vendors can’t treat security as something they hand off. You want duplicative layers of protection, not gaps where everyone assumes someone else has it covered.” For cybersecurity measures to be most effective, districts and vendors will have to work together—and many states are recognizing the challenges that now loom on the horizon. Matthew Given, CEO of Seesaw Learning, says, “We’re seeing more states move from recommendations to hard requirements around data privacy and security. In places like North Carolina, SOC 2 compliance isn’t optional anymore. It’s a gatekeeper for whether a product can even be used in schools.” States’ requirements will undoubtedly affect districts’ procurement choices in the present and into the future.

Detection Capacity Varies Widely by District Size

Districts have a role to play, but it might not be one they’re qualified for. Michael Klein says, “If you’re in a procurement process, you can and should ask relevant security questions. But vendors may not be able (or willing) to answer everything, and it’s not realistic to push full due diligence onto school districts. Functionally, we shouldn’t be asking districts with one IT staff member to evaluate the security posture of multi-million- or billion-dollar companies.” In this way, the relationship between districts and vendors may be slightly asymmetric, at least in terms of capacity when it comes to evaluating security. As Arman Jaffer says, “From a vendor perspective, the bar has to be higher, especially when you’re building tools that touch student data. Districts don’t always have the capacity to deeply evaluate security posture, so vendors need to assume that responsibility upfront, not wait to be asked.”

Still, both districts and vendors are doubtlessly operating to the best of their abilities. In fact, this rise in vendor-related incidents does not necessarily mean edtech tools have become less secure. Instead, it reflects how operationally and data-critical certain shared platforms have become. As districts consolidate student records, identity systems, and administrative workflows within a small number of widely used services, a single compromise can expose sensitive data across hundreds of districts at once.

When it comes to handling massive amounts of personally identifying information, vendors are under huge amounts of pressure. As Doug Levin sums up, “When schools complain about vendors and vendors complain about schools, it usually means we’re not talking to each other very well. The truth almost always lies somewhere in the middle.”

Note: This rise in vendor-related breaches – reflective of the wide-scale 2024 PowerSchool incident – does not indicate that edtech is becoming less secure; rather, it reflects the central role these platforms now play in school operations. As schools rely on shared systems, those systems become attractive targets, and strengthening safeguards and clear standards across the ecosystem is critical to reducing the impact of future incidents.

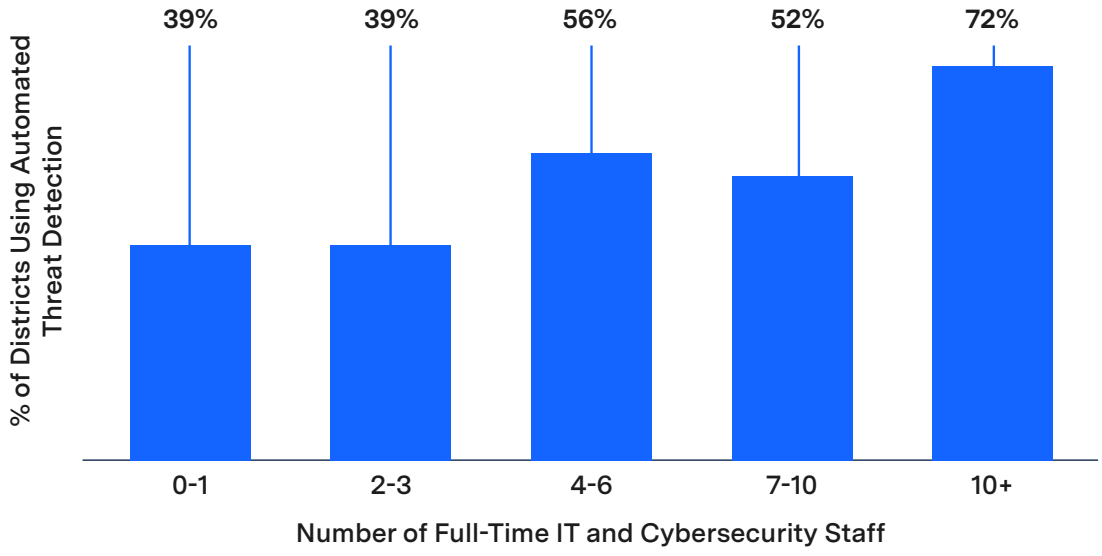
Districts’ ability to detect threats varies dramatically, often depending on staffing and capacity. Overall, 49% of districts use automated monitoring systems to identify suspicious activity, but that average masks significant disparities. In districts with 7-10 dedicated IT staff, automated monitoring adoption climbs to 72%, whereas districts with 0-1 IT staff lag at just 39%. Detection confidence reflects these gaps: 44% of districts believe they could detect a breach within hours, yet a concerning 17% are unsure of their detection capabilities entirely. In lower-resourced districts, detection is even more reactive, with 21% relying primarily on reports from staff, students, or families rather than proactive security tools to surface incidents.

Conclusion

Together, these trends signal a sector under sustained strain. Breaches are more frequent, more varied, and more entangled with third-party systems than ever before, and not all districts have the same capacity to see or respond to them. As incidents move from “likely” to “probable,” cybersecurity can’t remain a background concern or a once-a-year exercise; it becomes a core part of how districts design their systems, select partners, and allocate scarce resources.

Automated Monitoring Adoption by IT Staffing Level

Districts with more IT staff are far more likely to use automated threat detection



Clever

The Identity Gap That Still Hasn't Closed

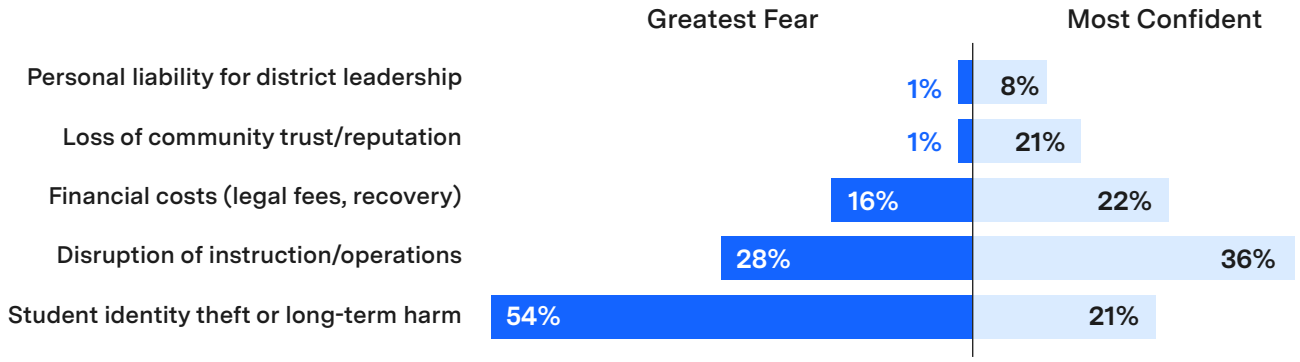
Last year's report highlighted student identity protection as the emerging frontier in K-12 cybersecurity, a space where risks were rising faster than safeguards. In 2026, that frontier remains unchanged. What has shifted is the visibility of the consequences: as threats to student identities intensify, the cost of failing to close this gap is becoming increasingly apparent. Districts overwhelmingly recognize student identities as the highest-stakes target, yet they continue to lack the systems, workflows, and guardrails needed to protect them effectively. Underlining this tension, Doug Levin says, "It's hard to argue that, as a whole, we are mature when it comes to cybersecurity. There's no federal regulation that really requires a duty of care for school systems or, arguably, for vendors either."

Student Identity Tops District Fears – But Not District Readiness

Districts now place student identity protection at the center of their cybersecurity concerns. When asked about the most feared outcome of a breach, 54% of leaders identify student identity theft or long-term harm as their number one worry. This concern far surpasses other risks: only 16% cite financial loss, 28% highlight operational disruption, and just 1% reference loss of community trust.

The message is unmistakable: leaders understand that exposing student identities carries a uniquely profound and lasting impact, one that can follow a child for years. Yet despite this heightened awareness, districts feel least confident about addressing the very risk they fear most. Only 21% say they are "most confident" managing student identity threats, while 36% feel most confident managing operational disruptions, which they view as more within their control. This mismatch between priorities and preparedness reveals a structural gap–not in awareness, but in capability.

The Preparedness Gap: What Districts Fear Most vs. What They Feel Ready For



If your district experienced a major breach tomorrow, how would you prioritize the following concerns? Please rank them from 1 (greatest immediate concern) to 5 (least immediate concern)?

Clever

The Student Authentication Challenge Sidebar: Student authentication is fundamentally different from adult authentication. Most security models are designed for users who can manage complex passwords, keep a single device, and reliably use MFA – none of which consistently holds true for kids. In classrooms, 25 students need to get online within seconds, often on shared devices that open and close dozens of times a day, which makes any added friction a nonstarter for teachers.

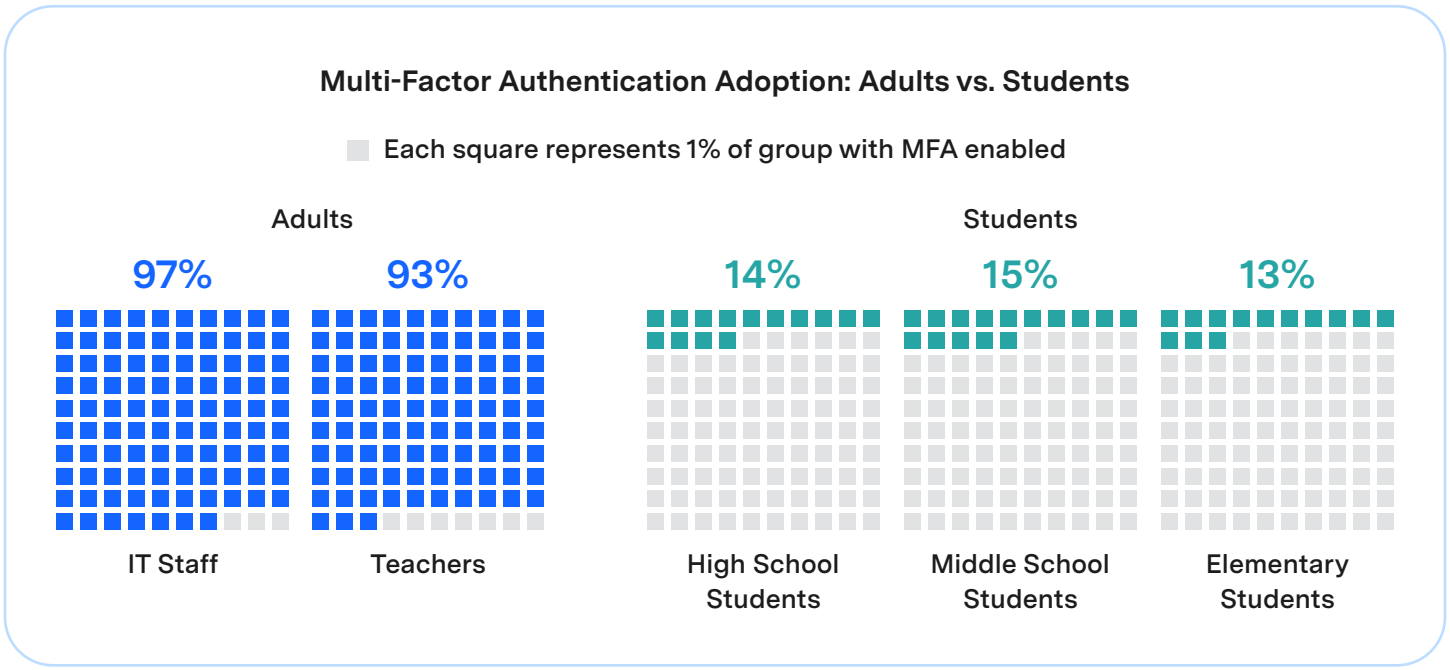
At the same time, common K-12 practices like using dates of birth as passwords, banning personal devices while expecting stronger authentication, and relying on adult-oriented tools like biometrics or passkeys all collide with developmental, logistical, and community concerns. The result is a persistent gap: schools know student accounts are a major source of risk, but the authentication tools built for the "real world" rarely fit the realities of schools.

Students Face the Steepest Compliance Challenges

Student identity protection requires systems-level coherence: consistent authentication, strong identity workflows, and age-appropriate security practices that many districts simply do not yet have. This misalignment becomes clearer when examining which groups struggle most with compliance. Students are identified by 36% of districts as facing the greatest challenges meeting security requirements, more than teachers (23%) or non-teaching staff (16%). The reasons vary, from limited device access and classroom constraints to policies like phone bans, but the effect is the same: students remain the least protected population in a system increasingly shaped by digital identities.

MFA Coverage Leaves Students Behind

However, nowhere is this challenge more visible than in MFA adoption. While 93% of teachers and 97% of IT staff use MFA, student coverage remains exceptionally low around 13% for all grades. These numbers have barely moved since last year despite growing threats, underscoring how difficult it remains for districts to implement secure, developmentally appropriate authentication practices for minors. In other words, the group with the highest exposure and the lowest ability to self-protect is also the group with the least comprehensive safeguards. Furthermore, some tools don't support MFA usage. As Corey Lee, Security CTO, of Microsoft SLED, explains, "What we're seeing across education is that open source tools, especially free or non-enterprise-grade ones, often don't support basic security controls like MFA. That creates real risk for districts, even when their core systems are well protected."



Clever

Internal and External Threats Converge on Student Accounts

Internal threats are also becoming harder to ignore. Student-initiated attacks are emerging as a growing internal risk, with student-on-student or student-on-staff hacks rising from 13% to 18% of incidents. At the same time, external cyberattacks specifically targeting student accounts increased from 26% to 32%, showing that students are being targeted both from inside and outside the system.

Conclusion

The persistence of this identity gap carries significant implications for the sector. As student accounts become more deeply connected to learning tools, assessments, communication channels, and high-value data, their exposure increases. Closing this gap will require solutions that work for students' realities, not adult workflows, and that reduce friction rather than creating new barriers. Protecting student identities isn't just a cybersecurity goal; it is foundational to building long-term digital trust within school communities. As Keith Krueger says, "When we ask districts how vulnerable they think they are, they consistently underestimate their risk, even though we know K-12 is one of the most targeted sectors."

While 93% of teachers and 97% of IT staff use MFA, student coverage remains exceptionally low around **13%** for all grades

MFA 2026 Snapshot: Progress Amid Persistent Challenges

Multi-factor authentication (MFA) is now widely used across K-12 schools, but adoption alone doesn't tell the full story. While most school organizations have implemented MFA for staff, uneven rollout, workflow friction, and misaligned policies continue to create gaps. In many cases, these challenges lead to insecure workarounds that weaken the very protections MFA is meant to provide.

Rapid adoption meets implementation reality

84% of school organizations have now implemented MFA, up from 77% in 2023, with particularly strong gains among teaching staff (80% to 93%) and non-teaching staff (75% to 89%). IT staff lead at 97% coverage.

Student adoption remains low

roll-out to K-12 students across all grade bands remains low with only 13% implementation; this is up 3 percentage points from 10% in 2023.

Yet implementation challenges persist

59% report teacher or staff resistance as their top MFA challenge, followed by technical/logistical difficulties (49%) and increased help desk burden (44%). Interestingly, 23% cite student mobile phone bans as limiting MFA options, highlighting how well-intentioned policies can conflict with security needs.

Despite MFA adoption, insecure practices remain rampant

62% of school organizations report staff and students writing down or insecurely storing login credentials, while 57% reuse passwords across systems. Password sharing affects 55% of school organizations, and 51% report use of simple, easily guessable passwords. Nearly half (48%) report staff using personal devices to circumvent IT's security controls.

Cyber Insurance: Driving Practice but Delivering Mixed Results

Cyber insurance has rapidly become one of the most influential forces shaping cybersecurity practice in K-12 schools. As the financial and operational stakes of cyber incidents rise, insurers have responded by tightening requirements and making coverage dependent on controls like MFA, identity management, training, patching, and vendor risk assessments. For many districts, these requirements may function as a de facto cybersecurity roadmap, yet the path to meeting them is often fragmented, confusing, and dependent on tools and processes that were not built for school workflows. In some cases, it may be completely uncharted territory. According to Doug Levin, “In the vast majority of states, individual school systems are left on their own to decide how to manage cybersecurity risk, or whether they even recognize it as something they need to manage.” Cyber insurance therefore gives districts an impetus to address these concerns that they may not have otherwise had.

How U.S. Cyber Insurance Works in K-12 Schools

1. **Cyber insurance is often confusing for districts** because they rarely interact directly with the insurance representatives who set coverage terms or security requirements. Instead, most districts begin by completing an application, usually handled by some combination of the CTO, business office, legal team, and a risk manager. This application asks for basic information about the district's size, revenue, and cybersecurity posture, including whether MFA is in place, how identities are managed, and what tools are used to monitor threats. Because **responsibility is fragmented across departments,** the person completing the form may not always have a full understanding of the district's technical readiness or the implications of certain answers.

2. Once the application is submitted, it is handed off to a broker. The broker (not the district) shops that application to multiple carriers, negotiates terms, and recommends which policy to buy. Most districts assume the broker and carrier are the same, but in reality they occupy very different roles: **the broker is a middleman, while the carrier is the entity that actually decides whether to insure the district and what safeguards must be in place before coverage can begin.**

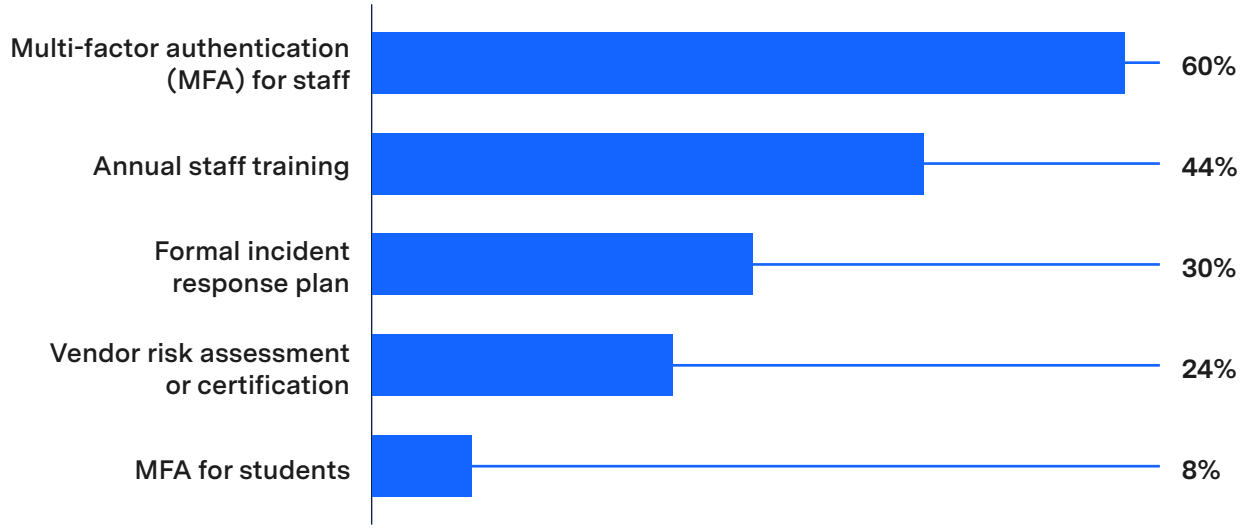
3. Carriers play the most consequential role. They determine premiums, set requirements, and often run vulnerability scans of district networks before approving coverage. In recent years, **carriers have increasingly required core identity safeguards, most commonly MFA,** identity management workflows, patching protocols, staff training, incident response plans, and vendor risk assessments. These requirements are not optional; districts must satisfy them within tight timelines or risk losing coverage.

4. If a breach occurs, control shifts once again, not to the district, but to the carrier. The carrier activates specialized "breach response" vendors, usually law firms and forensic investigators, who take over communication, analysis, and negotiations with attackers. Because this work happens under attorney-client privilege, and the client is technically the carrier rather than the district, **districts often have limited visibility into the details of what occurred or how it was resolved.** That lack of transparency leaves many leaders feeling uncertain about their own risk exposure even after the incident is closed.

5. Together, these layers – a fragmented internal process, broker intermediation, carrier requirements, and opaque breach response – create an insurance system that is hard for districts to navigate and even harder to translate into meaningful security improvements. And yet, because insurers now mandate the identity safeguards districts have struggled to implement on their own, insurance has become one of the strongest drivers pushing schools toward MFA, better identity management, and more consistent vendor oversight. In this way, **insurance doesn't just influence cybersecurity practice; it increasingly shapes the foundation of how districts secure access, protect data, and manage risk.**

What Cyber Insurers Require from Districts

Most common insurer requirements · Select all that apply



Insurance Mandates Reshape District Security Practices

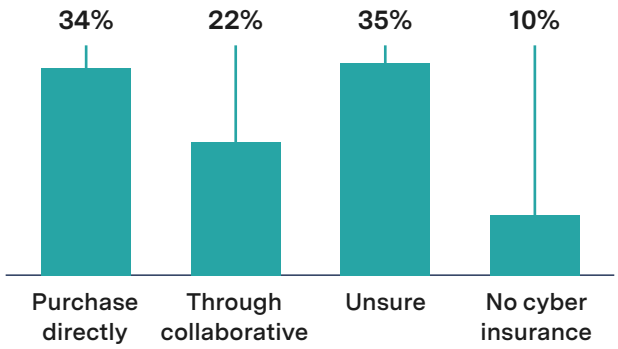
Insurance requirements are reshaping district security practices at scale. 58% of districts have adopted new technologies or processes specifically to comply with insurance mandates, and these mandates are increasingly tied to identity and access controls, the very foundation of most school cyber incidents. The most common insurer requirements include MFA for staff (60%), annual cybersecurity training (44%), formal incident response plans (30%), and vendor risk assessments (24%).

For many districts, these controls become urgent only when required by carriers, creating a reactive environment where coverage, not security, is the initial driver of change.

But meeting these requirements is not straightforward. The insurance market itself is fragmented: 34% of districts purchase coverage directly, 22% rely on collaboratives, and 35% are unsure how their coverage is even obtained. Nearly 10% of districts operate without cyber insurance, often because they cannot implement required safeguards in time or cannot interpret the technical obligations embedded in their policies. This complexity heightens risk, especially for smaller districts with limited IT staffing.

Cost pressures are also compounding the challenge. 32% of districts cite cost as their primary insurance concern, and pricing varies dramatically: 35% pay under $10,000 annually, while 8% pay more than $100,000. Carriers also impose different security expectations, leaving districts confused about which standards truly matter and how to prioritize their efforts.

How Districts Obtain Cyber Insurance Coverage



Clever

Compliance Doesn't Always Equal Confidence

Even after implementing new controls, many districts remain unsure whether insurance improves their security posture. Only 12% believe insurer-driven requirements have "significantly improved" their security, while 39% are uncertain. Notably, districts that avoided breaches were more likely to believe insurance improved outcomes (57%) than those that experienced incidents (44%). This suggests that compliance-driven implementations, especially MFA rollouts or vendor checks done quickly to satisfy a carrier, do not always translate into durable, everyday security practice.

A Governance Gap Slows Implementation

A persistent governance gap complicates this further. While insurance requirements directly affect technical systems, only 34% of districts have IT leaders managing their insurance relationship, compared to 46% where finance departments lead. This disconnect means decisions about MFA, identity systems, or vendor vetting may be made without the people responsible for implementing them, slowing progress and increasing risk.

Insurance as a Driver, But Not a Destination

Insurance has become a powerful driver of cybersecurity practice, but it has also exposed the difficulty districts face in rapidly meeting identity, access, and vendor security requirements with limited staff and fragmented systems. As insurers continue to tighten standards around MFA, identity management, and vendor oversight, districts increasingly need solutions that reduce complexity and make compliance achievable, without diverting attention from instructional priorities. It should be noted, however, that conditions (and the extent to which insurance affects how schools handle cybersecurity) vary based on location. Matthew Given explains: "The maturity of data privacy and security expectations varies widely around the world. Europe is at one end of the spectrum—highly restrictive and deeply scrutinized—while other regions are more focused on whether you meet baseline requirements and can clearly explain what you're doing."

Conclusion

Clever's role in simplifying identity workflows and supporting MFA adoption gives districts a clearer path to meeting insurer expectations while strengthening real security outcomes. In a landscape where insurance mandates are accelerating, tools that unify identity, access, and vendor controls are becoming essential—not just for coverage, but for resilience.

AI and Future Threats: An Unprepared Sector

In last year's report, we identified an emerging "AI security paradox": district leaders feared AI-driven threats, yet few had the safeguards or policies to manage them. In 2026, that paradox has sharpened into a dual challenge. AI is accelerating the speed, scale, and sophistication of external attacks. As Doug Levin explains, "AI has made phishing and social engineering more frequent, more targeted, and more sophisticated because the tools to do it are easier to use." At the same time, AI has expanded into the edtech tools districts rely on. As a result, schools now face risks from within and outside their tech stacks, but they scarcely have the capacity to evaluate AI as an embedded feature set in their existing apps, let alone as an attack multiplier.

On the other hand, despite the growing challenges AI creates, some districts see the **benefits of addressing cybersecurity threats with AI** itself, offering a more optimistic view of the role this technology is playing in schools.

AI Heightens Risk

Still, district anxiety about AI remains high. 81% of districts believe AI is heightening their cybersecurity risks, with 30% reporting "significant" increases in risk and another 50% reporting "somewhat" increased risk. At the same time, districts are confronting a second wave of AI exposure: the rapid expansion of AI inside instructional and operational tools. Yet only 11% of districts have a formal process to vet AI use in edtech products.

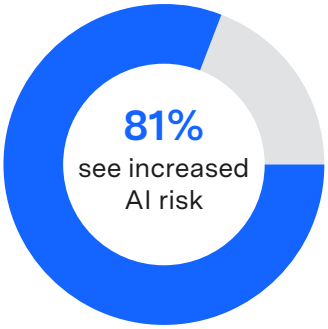
Another 36% rely on informal approaches, and 21% have no vetting process at all, meaning the majority of AI entering classrooms is adopted without structured review of privacy implications, data handling practices, or potential security risks. These internal exposures are very different from traditional cyber threats, but schools lack coherent frameworks to evaluate or monitor them. Corey Lee explains, "AI has dramatically increased data sprawl and access challenges. Many AI tools entering schools don't respect enterprise security standards, and that forces districts to make hard choices between innovation and risk."

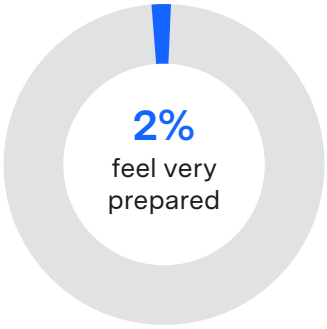
81%

of districts believe AI is heightening their cybersecurity risks

The AI Preparedness Gap

While district leaders believe AI is increasing cyber security, a majority feel unprepared for the risks





Districts Face a "Preparedness Cliff"

This combination of external AI-enabled attacks and internal AI-enabled tools has created what many leaders describe as a "preparedness cliff." When asked to look ahead three years, only 2% of districts say they feel "very prepared" for AI-related cyber risks. While 45% report being "somewhat prepared," a striking 38% say they are "not very prepared" (28%) or "not at all prepared" (10%). The gap between perceived risk and district readiness is one of the largest in this year's report.

AI is reshaping the cybersecurity landscape faster than districts can respond, expanding both the threat surface and the complexity of evaluating tools used in classrooms. According to Arman Jaffer, this dramatically ups the ante: "AI raises the stakes for trust. When you're using AI in classrooms, you're not just talking about functionality. You're talking about privacy, data flows, and whether educators feel confident that the tool is working in their best interest." In fact, the sector's preparedness gap reflects not a lack of awareness, but a lack of scalable, identity-centered guardrails that help districts understand who is accessing AI features, how data flows through systems, and which vendor practices can be trusted.

Calls for Transparency Grow Louder

It is not surprising, then, that 60% of districts strongly agree that policymakers should require clearer AI disclosures from vendors. Leaders are asking for transparency about how AI models function, what data they access, how outputs are controlled, and whether vendors have taken steps to mitigate misuse. Michael Klein explains: "We still don't know enough about how AI is being used, either on the attack side or the defense side. What's clear is that it has the potential to dramatically shift who has the capacity to attack school systems." When it comes to how AI operates in edtech tools, there is a defined information gap between what districts need and what vendors can provide.

In many cases, districts' call for transparency is driven not by fear of AI's instructional use, but by the operational reality that they cannot effectively evaluate risk without better information from their partners. While this transparency may not be a priority for most major tech companies, it is absolutely essential for schools. As Nicol Turner Lee, Director of the Center for Technology Innovation at Brookings, says, "Large companies are driven by profit. Security matters, but it's not always embedded as a core value in the same way it is for smaller, education-focused organizations."

Conclusion

As districts call for stronger transparency and more manageable frameworks for evaluating AI, solutions that simplify identity management, centralize access, and support consistent vendor vetting will become increasingly important. Addressing AI-driven threats will require not just new tools, but clearer structures for how people, data, and technology interact across the entire K-12 ecosystem.

The Resource Reality: Alignment Without Capacity

Across the country, district leaders increasingly understand what strong cybersecurity requires, and their priorities reflect a clear desire to strengthen defenses, but external realities prevent them from doing so. The problem is not a lack of awareness or a lack of will, but a lack of capacity. As threats grow more complex and identity systems become more central to school operations, districts are running into familiar limits: too few staff, too little time, and tools that are often difficult to implement or sustain. This gap between priorities and practical capacity is now one of the most defining challenges shaping K-12 cybersecurity.

Staffing and Budget Shortfalls Remain the Top Barriers
Resource limitations continue to outpace every other barrier districts face. 36% of districts cite a lack of dedicated cybersecurity staff as their top challenge, up from 32% last year, making it the most significant and persistent obstacle to progress. Budget pressures follow closely, with 27% pointing to financial constraints (up from 23% in 2023). In contrast, only 11% of districts say leadership support is a top challenge, signaling that buy-in is no longer the primary barrier. Instead, awareness has grown faster than the resources necessary to turn that awareness into action.

Priorities Reflect Ambition – Constrained by Reality
These constraints directly shape how districts plan for and prioritize future improvements. Looking to 2026, leaders' top cybersecurity priority is improving threat detection and monitoring capabilities (34%), followed by expanding MFA coverage (20%) and increasing staff training (15%). These are foundational steps toward a more resilient security posture but each requires staffing, sustained operational capacity, and tools that are easy enough to implement widely and maintain over time.

Clever

Districts Choose Practicality Over Sophistication

Districts' evaluation criteria for new security tools reinforce this reality. When selecting technology, 76% of leaders prioritize cost, 72% prioritize ease of use for staff, and 62% prioritize security strength. Practicality consistently outweighs sophistication; districts will choose the solution they can implement reliably, not the one with the most advanced features. According to Corey Lee, the answer may be simplification: "Many districts are operating in incredibly complex environments with limited staff. Simplifying architecture and reducing tool sprawl is often the most realistic way to improve security without adding headcount." This is not a lack of ambition on the part of districts. It is a reflection of the operational realities in K-12, where IT teams are often small, overextended, and responsible for supporting a vast and evolving ecosystem of devices, applications, and users. As Doug Levin explains, "Any Fortune 500 CISO dropped into a large school district would be blown away by how many tools and systems are in use, and they would never design something that complex or decentralized from scratch."

When coupled with sprawling systems, these resource constraints don't just slow cybersecurity progress. They also shape the types of tools and safeguards districts can realistically adopt in the present tense. Levin says, "In education, the number of people and devices IT staff are responsible for is orders of magnitude higher than in other sectors. One IT person may be responsible for 1,200 users. That level of staffing wouldn't be acceptable anywhere else." When time, staffing, and budgets are limited, districts need security solutions that reduce complexity, streamline identity workflows, and strengthen protection without demanding significant new capacity.

As threats escalate and expectations rise, success will depend as much on simplicity and scalability as on sophistication. In a landscape where awareness is high but capacity is low, tools that make strong security easy to implement and maintain will have the greatest impact. And one unexpected outcome of an ever-rising number of incidents is increased preparedness. As Cynthia Hays, Director of Risk Management at Oklahoma City Public Schools, says, "We know incidents are going to happen. The difference now is that we've built processes, relationships, and muscle memory around responding—with legal, IT, and vendors all working together instead of scrambling in isolation."

Top cybersecurity challenges

36% lack of dedicated staff

27% financial constraints

Conclusion

AI is forcing schools to confront cybersecurity in ways they never had to before. Every new tool raises questions that districts once reserved for IT teams alone: What data does this system touch? Who can access it? What happens if the system fails? In practice, this means cybersecurity is no longer confined to back offices or incident response plans. It is becoming part of everyday decision-making across classrooms, central offices, and leadership teams.

The importance of these day-to-day choices has been heightened with the rapid onslaught of AI-powered apps and tools. Districts cannot realistically block AI from entering schools, nor can they manually vet every new application. **Building roadblocks isn't the answer. Instead, establishing clear, scalable guardrails, or simple rules around identity, access, data flows, and vendor expectations that allow innovation to move forward safely, is the challenge ahead.** These "fences" don't slow progress; they make it possible to sustain it.

In this way, AI is becoming an unexpected instructor. As districts wrestle with managing risk, they are also teaching students, staff, and future graduates what responsible digital participation looks like: how access is managed, why privacy matters, and how security enables trust rather than restricting it. From early lessons about safe logins to advanced engagement with real-world security policies, schools are shaping a generation that understands cybersecurity not as a technical afterthought, but as a shared responsibility.

The findings in this report point to a sector at an inflection point: highly aware of its risks and increasingly aligned on priorities, but constrained by capacity and complexity. The path forward is not more fear, more friction, or more fragmented controls. It is clearer structures, simpler systems, and identity-centered foundations that let schools innovate securely today to prepare students for the workforce they will enter tomorrow.

Top Cybersecurity Priorities for 2026

What IT leaders are focusing on this year

34%

Improving Threat Detection & Monitoring

Real-time systems that spot suspicious activity before it becomes a breach

20%

Expanding MFA to More Users

Requiring a second verification step (like a code or app) to log in

15%

Increasing Cybersecurity Training

Teaching staff and students to recognize phishing and other threats

10%

Strengthening Data Governance

Better controls over who can access sensitive student information

9%

Enhancing IT-Finance-Leadership Collaboration

Breaking down silos so security decisions involve the right people

5%

Improving Vendor Risk Management

Vetting third-party tools and their AI features before adoption

2%

Implementing Zero Trust

Verifying every user and device, every time, regardless of location

2%

Reducing Insurance Costs

Meeting insurer requirements to lower premiums and maintain coverage

Clever

AUSTRALIA OVERVIEW

Cybersecure 2026 Report

CLOSING THE IDENTITY GAP FOR GLOBAL EDUCATION

Executive Summary

Australian schools are treating cybersecurity as a planned, ongoing responsibility rather than just reacting when problems occur. Australian schools show a well-developed and structured approach to cybersecurity. This is reflected in their early alignment with recognised national and international frameworks and in the active involvement of school leadership and governing bodies. Cybersecurity is no longer approached through isolated incident response but is framed as an enterprise-level and child safety concern. Schools are guided by multi-year uplift strategies aligned with frameworks such as the Essential Eight Maturity Model[1] and ISO 27001, a widely recognised international information security management standard.

National reports tend to focus on the high-impact threats like ransomware and Business Email Compromise (BEC), but evidence consistently pointed out a more persistent reality that phishing is still the primary way these incidents start. This risk has intensified as AI-generated content makes phishing emails more convincing and harder to detect. According to the CyberCX 2025 Threat Report, education accounted for 8 percent of reported cyber incidents across industries in 2024, placing the sector just behind healthcare and financial services[2].

Australia stands out for its early and consistent adoption of established cybersecurity frameworks. This progress has been largely driven by steady, top-down governance; however, leaders are now flagging a growing strain on staff capacity and overall organisational resilience as they try to keep up the pace.

What this means for schools

Schools are developing a greater understanding of what is happening in classrooms, recognising the emerging needs of teachers and the importance of strong leadership teams who can identify and respond to matters early.

There is also growing recognition of the importance of trusted partners who can truly support schools in navigating complexity. Leaders are beginning to build a shared language and more predictable processes that strengthen alignment across the community.

For teachers, this means clearer expectations and greater consistency. For boards, it provides heightened visibility and informed oversight. For students, it reinforces the connection between digital safety and protection. This helps to create more secure and helpful learning environments.

Key takeaway

Stronger accordance with frameworks and clearer governance ownership are helping Australian schools strengthen their cyber maturity. The next challenge will be maintaining momentum while balancing staff capacity and the speed of organisational change.

Identity, Access, and User Behaviour

In Australian schools, identity is treated as the primary control surface for reducing cyber risk. For Australian schools, identity is now seen as the primary frontline. While phishing remains the most frequent way attackers get in, the rise of AI-generated content is making these attempts much harder for staff to spot. In response, schools are moving beyond basic security and doubling down on mandatory MFA, stricter access controls, and a more rigorous approach to system permissions.

> "MFA for staff was the first control we put in place. It is an easy win."
>
> **Adam Bird** | Information and Communication Technology (ICT) Director, Hunter Valley Grammar School (New South Wales)

While MFA for staff is now standard practice, applying it to students is far more complicated. Between age-related hurdles and the reality of device access, a one-size-fits-all approach just doesn't work. Instead, schools are leaning on "defence in depth", combining monitoring and safeguarding frameworks rather than relying solely on login requirements.

Even with strong tech, basic staff habits, like leaving devices unlocked or sharing screens, are still a significant weak point. However, leaders are quick to point out that this isn't usually malicious. More often, staff are simply working around clunky system designs to keep a lesson moving. This draws attention to the need for security approaches that fit with classroom practice.

Ultimately, leaders agree that controls must be proportional to the user's age and situation, focusing as much on oversight and impact as on technical barriers. Implementing cybersecurity in schools is a balancing act that changes with the age of the student. In early years settings, complex authentication can quickly turn into an impediment, taking away precious instruction time. For older students, the goal is to foster independence without sacrificing safety.

However, there is a deeper tension: visibility. Safeguarding teams need to be able to spot unusual behaviour or access issues. This becomes impossible if security protocols are heavy-handed, obscuring what is actually happening. Effective protection has to be transparent enough to keep student wellbeing priority.

What this means for schools

Australian school leaders increasingly view the human factor as an element to design for, not simply a problem to solve. They recognise that when security measures are complex or disrupt teaching, educators may bypass them. The focus has shifted from enforcing strict controls to creating systems that integrate smoothly into school routines. The aim is to support teachers while ensuring student safety in digital environments. By prioritising user experience, schools are enhancing security without compromising learning or relationships.

Key takeaway

Identity controls work best when they make sense in everyday practice and do not interrupt the flow of school life. In Australia, leaders are concentrating on safeguards that are proportionate and workable in real classrooms. This is important so that security can be strengthened without placing extra strain on staff or interrupting students' learning.

Governance, Insurance, and Accountability

Cybersecurity is continually being treated as a school governance responsibility rather than a technical function. Strategic direction typically sits with senior ICT leadership but is supported by school level governance structures and board awareness. Regulatory obligations, in particular under the Notifiable Data Breach Scheme[3], have elevated cyber risk into board level discussions and driven the development of formal incident response playbooks and escalation pathways.

> "It is not an IT problem; it is a whole school problem. You need buy in from leadership and your governing body."
>
> **Adam Bird** | Information and Communication Technology (ICT) Director, Hunter Valley Grammar School (New South Wales)

Framework alignment plays an important role in governance. Schools describe frameworks such as the Essential Eight and ISO 27001 not as compliance checklists, but as organising structures that help identify priorities and establish shared language. This approach supports more sustained improvement across leadership, IT, and operational teams.

Insurance requirements are increasingly shaping governance practice, with evidence of controls and incident readiness becoming baseline expectations.

What this means for schools

In many Australian schools, conversations about cybersecurity are happening more regularly with technical teams. Leaders are bringing these discussions into leadership meetings and board conversations because they are recognising that cyber risk is closely connected to safeguarding, organisational resilience, and the everyday functioning of the school. For many, this has meant slowly shifting the mindset. **Leaders are asking who owns the risk and how decisions are shared, rather than who manages the technology.** This increased attention can feel demanding, but it is also helping schools move towards clearer roles, stronger collaboration, and more confident leadership around complex challenges.

Key takeaway

Legal expectations and insurance requirements are reinforcing this shift, encouraging schools to embed cybersecurity into regular governance practices and recognise it as an ongoing leadership responsibility that supports the safety and stability of the whole school community.

AI as a Risk Multiplier

Artificial intelligence is not viewed as a separate category of risk, but as a factor that intensifies existing vulnerabilities. Leaders report that phishing and impersonation attempts are more convincing, faster to deploy, and harder for staff to identify.

> "It is ever changing. You cannot remain complacent."
>
> **Adam Bird** | Information and Communication Technology (ICT) Director, Hunter Valley Grammar School (New South Wales)

AI enabled tools also expose weaknesses in access architecture. Where permissions are poorly designed, AI systems tend toward openness, making unintended data visibility more obvious and more consequential. **As a result, leaders emphasise verification practices, disciplined access design, and more deliberate decision-making, instead of pursuing outright bans on AI.**

Change fatigue is emerging as a secondary risk. Leaders note that the challenge is increasingly one of pace rather than awareness. This requires careful change management and ongoing consultation with staff.

What this means for schools

For many school staff, the effects of AI are felt in everyday moments. Emails look more professional. Messages sound urgent. It is becoming harder to judge what is real at first glance. Leaders are starting to see that this is not only a technical challenge, but a human one.

Instead of shutting systems down, many schools are concentrating on practical habits. **Staff are encouraged to pause, double check requests, and be clear about where to raise concerns.** The focus is on steady routines that fit into busy school days. These habits help protect sensitive information and reduce the risk that communication with parents is disrupted or misused.

Key takeaway

AI is increasing risk mainly through identity and human judgement. Schools are responding by strengthening verification practices and clearer access discipline, rather than relying solely on adding more tools or restrictions.

Implications for international schools operating in Australia

In the Australian context, the perception of cybersecurity has shifted. It is no longer framed as a specialised technical niche, but as a fundamental requirement for regulatory credibility. Leaders featured in this report discussed robust security is now "table stakes", inextricably linked to a school's safeguarding obligations. **Ultimately, a school's ability to prove it is operating responsibly now hinges on two things: visible accountability from the top and a clear alignment with established security standards.**

Evidence suggests that progress is shaped less by the number of tools in place and more by clarity around identity controls and access design. Ongoing organisational dialogue about risk also plays an important role.

> "You can have all the policies and systems in the world, but connection and regular conversation will win every time."
>
> **Matt Esterman** | Senior Digital and Cybersecurity Leader (Australia)

Embedding cyber awareness into everyday practice is no longer optional. **Schools that treat security as a cultural priority rather than a technical one are far better equipped to handle AI-enhanced risks while proving their commitment to safeguarding to parents and regulators alike.**

What this means for schools

Many international school leaders describe their role as balancing two sets of expectations at once. They are part of global networks and often use international platforms, yet they answer directly to local regulators and families who expect clear assurance that children are safe. While digital risks become more visible, leaders are taking a more open and active stance on cybersecurity. It is no longer confined to technical discussions; it features in routine leadership meetings and strategic planning and is often linked to recognised standards. This more visible ownership signals to parents and governing bodies that digital safeguarding is being treated with the same seriousness as academic quality and student wellbeing.

Key takeaway

Schools that weave cybersecurity into governance, daily routines, and school culture tend to be better placed to maintain trust and respond to evolving risks, including those connected to AI.

Clever

CANADA OVERVIEW

Cybersecure 2026 Report

CLOSING THE IDENTITY GAP FOR GLOBAL EDUCATION

Executive Summary

Canadian independent and international schools have a difficult situation as they face enterprise-level cybersecurity risk while operating with capacity more comparable to small organisations. This comparison to small organisations refers to the breadth of systems, data types, and regulatory obligations involved, rather than institutional scale or staffing levels. Leaders featured in this report highlight a structural mismatch between responsibility and resourcing. Schools are managing complex data environments, extensive vendor ecosystems, and rising regulatory expectations with small IT teams and limited planning horizons.

Cyber and privacy risk are now understood as leadership and governance issues, rather than matters for IT teams alone. The interview evidence highlights social engineering, third party vendor exposure, and the growing use of AI-enabled impersonation as the main sources of risk. As traditional perimeter controls become less effective, leaders are placing greater emphasis on governance, identity management, and staff awareness as practical ways to reduce exposure

Regulatory scrutiny on schools is particularly high. At the federal level, compliance is shaped by the Personal Information Protection and Electronic Documents Act (PIPEDA)[4], as well as the additional provincial requirements such as Alberta's Personal Information Protection Act[5] and British Columbia's Freedom of Information and Protection of Privacy Act[6]. Collectively, these frameworks set higher standards for how personal data is handled and how breaches must be reported. For schools that already hold large volumes of highly sensitive information, this significantly increases legal and financial exposure

Note: In this report, we have references to "small" organisations which reflect school contexts enrolling approximately 800–900 students and often operating with fewer than 5–8 dedicated IT or digital staff. This illustrates the scale and capacity constraints discussed throughout the Canada findings.

What this means for schools

For many Canadian leaders, this is a constant balancing act. Executives are tasked with meeting high regulatory standards while steering small teams that lack a deep bench of specialists. This pressure trickles down into every decision: the pace of long-term planning, the depth of vendor vetting, and the way risk is translated for boards and families. In this way, cybersecurity is no longer an abstract compliance issue. It has become a fundamental test of capacity and professional responsibility.

Key takeaway

Canadian schools are reinforcing governance and identity controls, but limited internal capacity continues to shape the pace and depth of cyber progress.

Clever

Identity, Access, and User Behaviour

Leaders featured in this report consistently identify digital identity as the main point of entry for cyber incidents in Canadian schools. Social engineering is described as the most reliable intrusion method, reflecting a focus on exploiting human judgement rather than system vulnerabilities. Leaders note that phishing, impersonation, and related tactics have become harder to recognise, particularly as AI increases both their realism and speed.

Traditional perimeter controls are widely seen as less effective in today's school environments. Boarding settings, one-to-one device programmes, and higher levels of student autonomy make it difficult to rely on network-based defences alone. Students can easily bypass institutional controls through personal hotspots or unmanaged devices, which has led many leaders to place greater emphasis on identity-first security approaches.

> "[Students] can always hotspot… and bypass everything that you've put into place."
>
> **Bruno Petitti** | Executive Director of Digital Strategy, Ridley College (Ontario)

Multi-factor authentication (MFA) is now widely in place for staff. This reflects a shared understanding that staff accounts present the most immediate risk. **Student use of MFA, however, remains uneven and is shaped primarily by age considerations, device access, and school policies on mobile phone use rather than by a lack of awareness of risk.**

What this means for schools

When Canadian leaders talk about identity, they are not talking about a setting buried inside a system dashboard. They are describing how people actually work. The teachers move quickly between lessons and platforms. The students log in from different devices and locations. Many requests are answered on the assumption that the sender is known and trusted. **With this context, identity controls only work if they are clear, repeatable, and supported by ongoing training.** If they feel the controls are more complicated or disconnected from daily routines, they are likely to be bypassed.

Key takeaway

In Canadian schools, strong and usable identity controls are now the most reliable defence as traditional perimeter protections continue to weaken.

Governance, Insurance, and Accountability

The leaders who contributed to this report are explicit that cyber and privacy risk can no longer be delegated or outsourced. Accountability remains with the school, even when services are delivered by third-party providers. This reality is reshaping governance conversations, procurement practices, and board level oversight.

> "Cyber and privacy risk is no longer just an IT risk."
>
> **Chris Dale** | Director of Security Services, Educational Collaborative Network Ontario (Ontario)

A rising concern among IT leaders is vendor breaches. While privacy commissioners report rising third party breaches, school leaders bear the operational and reputational fallout. They are responsible for breach notification, parent communication, and regulatory engagement even when incidents originate outside their direct control.

Cybersecurity planning horizons tend to be short. Leaders describe cybersecurity approaches that are revisited every six to eight months. These are shaped by both the speed at which threats evolve and the limits of internal capacity. Insurance expectations and regulatory scrutiny further encourage a focus on demonstrable controls and active oversight, rather than reliance on policy documentation alone.

What this means for schools

The vendor might be the source of a breach, but the school owns the fallout. Boards, not third-party providers, are the ones pressured to explain what went wrong. These moments tend to redefine a leader's approach to everything from contract negotiations to how early they involve governors in digital strategy. Over time, the mindset shifts. **Schools are beginning to see that vendor risk is not just an IT problem; it is a core leadership responsibility where trust and accountability are constantly on the line.**

Key takeaway

In Canada, reliance on external providers is reshaping governance conversations, placing greater emphasis on oversight, contractual clarity, and clear leadership accountability.

AI as a Risk Multiplier

Artificial intelligence is widely described as accelerating existing threats, rather than introducing an entirely new category of risk. Interviewees highlight the growing prevalence of deepfake audio, automated phishing, and AI-assisted impersonation, which undermine traditional trust-based verification methods.

> "These actors are always coming up with new clever ways and they're using the tools faster than we are."
>
> **Bruno Petitti** | Executive Director of Digital Strategy, Ridley College (Ontario)

Leaders note that attackers now require minimal information to impersonate trusted individuals convincingly, increasing the likelihood of successful fraud and data compromise.

As a result, identity governance is increasingly treated as a leadership responsibility. Now, greater emphasis is placed on slowing decision-making and strengthening verification processes. This is paired with encouragement to escalate concerns, rather than relying solely on technical detection.

What this means for schools

In practice, this shift often comes up in small moments. For example, a finance officer receives what seems to be a routine request from a senior leader. Or a teacher answers a call from someone who sounds confident and familiar. Nothing about these situations feels obviously wrong. However, the pressure to respond quickly is still there. Canadian leaders describe how they are trying to change that instinct. They are encouraging staff to pause, question, and verify, even when a request appears legitimate. Over time, this builds a culture where double checking is seen as responsible rather than inconvenient.

Key takeaway

As AI becomes more convincing, Canadian schools are working to embed verification practices and shared accountability into everyday practice.

Implications for international schools operating in Canada

For international schools operating in Canada, cybersecurity risk is heightened by heavy reliance on third party vendors, expanding digital identities across platforms, and the use of global systems within a locally accountable regulatory environment. While platforms and service providers may operate internationally, accountability for data protection and breach response remains firmly local.

> "While school boards can outsource services, accountability can never be outsourced."
>
> **Chris Dale** | Director of Security Services, Educational Collaborative Network Ontario (Ontario)

Interview evidence suggests that effective cybersecurity in this context is shaped less by the volume of tools in place and more by governance maturity, disciplined identity and access management, and organisational culture. Leaders point to treating identity as a foundational control, supported by ongoing staff awareness and clear leadership ownership, as central to reducing exposure in internationally connected school environments.

What this means for schools

For international schools, the risk is layered. Most rely on global platforms based thousands of miles away, yet when a system fails, it is the local leadership team, not the provider, who is on the hook with parents and regulators. Managing that disconnect is a delicate task. **Leaders are now looking much closer at their vendor ties and pinning down exactly who gets notified during a crisis and when.** Ultimately, the focus has shifted. It is less about the software itself and more about a visible, local show of ownership.

Key takeaway

In Canadian international schools, strong governance ownership and disciplined identity management carry more weight than simply adding new tools or platforms.

Clever

UNITED KINGDOM OVERVIEW

Cybersecure 2026 Report

CLOSING THE IDENTITY GAP FOR GLOBAL EDUCATION

Executive Summary

The United Kingdom stands out for the intensity and consistency of cyber pressure facing its schools

Evidence from this region provides the clearest illustration of sustained, real-world cyber strain. **Leaders describe a threat environment marked by frequent phishing attempts, credential harvesting, ransomware incidents, and third-party platform failures.** These risks are no longer occasional events. They are embedded in the everyday operating reality of UK schools.

National authorities and school leaders report weekly intrusion attempts, with incidents ranging from harvested staff credentials to failures in third party systems such as payment platforms. Phishing remains the most effective attack vector, a finding reinforced by the National Cyber Security Centre[7] and echoed across all interviews. Despite expanded training efforts, human error remains the primary vulnerability, particularly as AI-generated emails become increasingly convincing and difficult to detect.

Cybersecurity has consequently become a permanent governance concern. Boards and proprietors now engage more regularly with cyber risk, incident readiness, and compliance obligations. However, overall cyber maturity across the sector remains constrained by funding limitations, ageing infrastructure, and limited access to specialist expertise. Leaders increasingly acknowledge that incidents are likely to occur, prompting a gradual but notable shift away from prevention alone toward resilience, incident response, and recovery planning.

What this means for schools

For UK schools, cyber pressure feels immediate and ongoing. Leaders are dealing with a steady stream of alerts and risk registers that require near-constant attention. This atmosphere dictates daily routines as much as any official manual. Now, boards are looking past simple compliance; they want to see resilience. The strategy has shifted accordingly. The focus is less on building a perfect fortress and more on ensuring the school can respond with a level head when something happens.

Key takeaway

In the UK, sustained threat exposure has placed resilience and visible governance ownership at the centre of cybersecurity strategy.

Clever

Identity, Access, and User Behaviour

Across the UK interviews, human behaviour is consistently described as the main source of vulnerability. Phishing is reported as persistent and high in volume, with leaders noting regular attempts throughout the school year. Despite increased awareness efforts, staff continue to be caught off guard.

> "The biggest risk is somebody clicking onto something they shouldn't have clicked onto."
>
> **Nicholas Little** | Head of School, International School of Aberdeen

AI generated content has reduced the effectiveness of traditional red flags, increasing the cognitive load on staff and narrowing the margin for error. This aligns with findings from the SANS Security Awareness Report, which indicate that social engineering and phishing account for approximately 80 percent of incidents involving human-related risk[8].

Multi-factor authentication for staff is now widely in place across UK schools and is generally treated as a baseline requirement, particularly for email and cloud-based services. This points to a common understanding that staff accounts present the most immediate exposure. The use of MFA for students remains uneven and difficult to apply consistently, shaped by age-related considerations, safeguarding priorities, and practical constraints around device access.

Evidence also highlights the compounding risk created by broad internal access within management information systems and integrated platforms. Where access rights are widely distributed, a single compromised account can expose large volumes of sensitive data.

What this means for schools

Across the UK interviews, a familiar story repeats itself. A message arrives that looks legitimate. An account has broader access than anyone realised. A routine click sets off a chain of events. Leaders are clear that these incidents rarely begin with a dramatic system collapse. They begin with everyday actions under time pressure. **In schools where access permissions are wide and roles overlap, the impact of a single mistake can spread quickly.** This is why so much attention is now being given to simplifying permissions, tightening identity controls, and making safe behaviour the easiest option.

Key takeaway

In UK schools, reducing unnecessary access and strengthening identity controls remain the most effective and practical ways to lower overall cyber risk.

Governance, Insurance, and Accountability

Cybersecurity in the UK is increasingly understood as a governance responsibility rather than a purely technical function. Interviewees consistently describe cyber risk as a standing item on organisational risk registers, reviewed at board or proprietor level.

> "Cybersecurity would feature fairly highly and permanently on that risk register."
>
> **Al Kingsley, MBE** | Group CEO, NetSupport and Multi Academy Trust Chair (UK)

This shift in governance responsibility has been further shaped by sustained regulatory pressure. UK GDPR, Information Commissioner's Office enforcement expectations[9], Keeping Children Safe in Education (KCSIE) guidance, the Online Safety Act[10], and the National Cyber Security Centre Board Toolkit[11] together establish a high threshold for accountability. The subject Access Requests are also increasing in both volume and complexity, requiring substantial staff time and more structured processes.

Despite rising expectations, leaders consistently identify funding as the defining structural constraint. Budget constraints limit the replacement of legacy systems, the recruitment of specialist expertise, and the adoption of more advanced preventive controls.

Insurance requirements also influence practice, with cyber policies increasingly requiring clear evidence of staff training, backup maturity, and documented incident response arrangements. In response to this, schools tend to focus on demonstrable baseline controls rather than more aspirational security models.

What this means for schools

Cybersecurity now appears regularly on board agendas in UK schools. Governors are asking sharper questions, and compliance requirements are more detailed. However, leaders also describe working within tight budgets and ageing systems. The ambition to improve is there, but capacity does not always match expectation. This creates a steady tension. **Decisions about upgrades, staffing, and external support must be weighed carefully against other school priorities.** Governance involvement is stronger than before, but the pace of change is often shaped by financial reality.

Key takeaway

While governance maturity continues to grow in the UK, budget constraints remain a significant factor in determining how far technical defences can progress.

AI as a Risk Multiplier

Artificial intelligence is accelerating the speed and sophistication of cyber incidents in UK schools.

The interview evidence shows that **artificial intelligence is not viewed as creating a wholly new category of risk, but rather as amplifying existing threats.** Leaders report that phishing emails are more convincing, impersonation escalates more quickly, and attackers move faster from credential compromise to data exfiltration.

Schools have expressed concern about AI bypassing filters, automating phishing, and intensifying safeguarding and academic integrity risks. Their responses are varied, from locking down AI access entirely to funnelling usage through controlled pathways.

> "We're not in a position where we can confidently allow AI… so we locked everything down."
>
> **James Clarke** | Director of Digital Strategy

Leaders are less inclined to pursue outright bans on AI and instead focus on applying existing safeguarding and data protection judgement. This approach is most evident where AI tools interact with sensitive student or family data.

What this means for schools

Several UK leaders describe how the timeline of an incident has shortened. It often starts with a single, believable email; before the IT team even flags a problem, credentials are gone and the breach is already spreading. That window for containment has essentially slammed shut. At the same time, safeguarding leads are wrestling with the messy reality of student AI use and the monitoring headaches that come with it. These are not separate departmental issues anymore, they have collided. **It is forcing IT, safeguarding, and senior leadership into the same room to build a unified strategy, whether they are ready or not.**

Key takeaway

As AI accelerates existing threat patterns, UK schools are tightening verification practices and strengthening collaboration between cyber, safeguarding, and governance teams.

Implications for international schools operating in the UK

International schools in the UK face heightened reputational exposure alongside regulatory pressure.

International schools operating in the UK face elevated exposure due to fee sensitivity, reputational considerations, and a heavy reliance on digital platforms. Interviewees note that incidents involving safeguarding data, early years information, or family records can quickly **undermine trust and have lasting implications for enrolment and community confidence.**

> "Nurseries have been blackmailed… threatening to release children's data."
>
> **Chris Beddows** | Headteacher, Dwight School London

While some international schools may benefit from stronger funding positions, leaders consistently note that behavioural risk and third party dependency act as equalising factors across the sector.

UK interview evidence frames resilience as an operational requirement rather than a strategic choice. Schools that plan explicitly for incidents and invest in preparedness, response, and recovery are better placed to navigate sustained cyber pressure within an increasingly complex regulatory and threat environment.

What this means for schools

For international schools in the UK, reputation sits close to the surface. **When families are paying premium fees, they do not just expect high-level safeguarding, they want proof of it.** When an incident occurs, the response is visible and personal. Leaders are acutely aware of how quickly a vague email or a shaky response can tank parental confidence. This means that resilience is not only about systems. It is about whether the board is ready, the staff are trained, and the leadership has a battle-tested plan for when things go wrong.

Key takeaway

To sustain trust, international schools in the UK must anchor cybersecurity in strong governance ownership, ongoing staff training, and well-rehearsed incident response.

References

[1] https://www.cyber.gov.au/business-government/asds-cyber-security-frameworks/essential-eight

[2] https://cybercx.com.au/news/cybercx-2025-threat-report-media-release/

[3] https://www.oaic.gov.au/privacy/notifiable-data-brehesac

[4] https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/

[5] https://kings-printer.alberta.ca/1266.cfm?page=P06P5.cfm&leg_type=Acts&isbncln=9780779831927

[6] https://www.bclaws.gov.bc.ca/civix/document/id/complete/statreg/96165_00

[7] https://www.ncsc.gov.uk/

[8] https://www.intelligentcio.com/me/2025/08/18/sans-report-finds-humans-still-the-main-attack-vector-as-80-of-organisations-flag-social-engineering-as-their-number-one-risk/

[9] https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/

[10] https://www.gov.uk/government/publications/keeping-children-safe-in-education--2

[11] https://www.ncsc.gov.uk/collection/board-toolkit