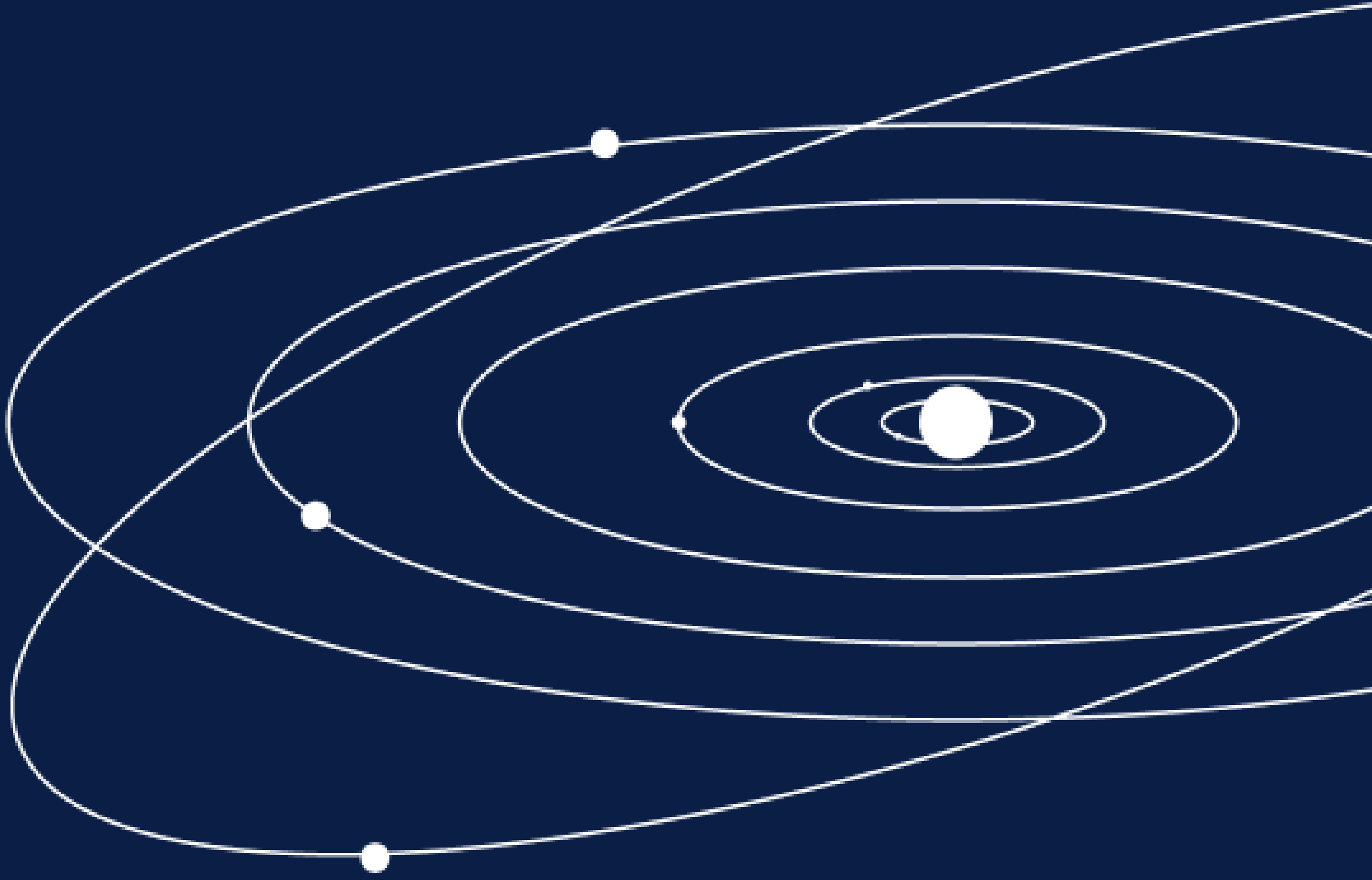
# From “No” to “Know”: How Technology Leaders Can Empower Digital Learning and Protect Student Identities



Produced by

Whiteboard Advisors

Commissioned by

Clever

# Foreword

## *By Mark Racine, Former Chief Information Officer, Boston Public Schools*

Like nearly every other aspect of our world, K-12 school systems run on connected technology. They rely on this technology to collect the data that they report to state and federal officials, communicate and share resources with staff and families, manage day-to-day work flows, and support educators in instructional delivery to students. This reliance on technology did not happen overnight, but it did happen relatively quickly. While many district leaders have made gradual transitions toward more-connected systems since the 2010s, COVID-19 turned those incremental steps into an all-out sprint. As the pandemic led to widespread school closures, districts that had been largely self-contained found themselves rapidly adopting new devices and applications to ensure students could continue to learn remotely. What began as an emergency response has since become a permanent transformation of how schools operate.

School systems' shift from analog to digital is visible in the things they buy, and importantly, in the ways they are organized. Senior-level education technology positions — often chief technology officers (CTOs) or chief information officers (CIOs) — have proliferated in school systems across the country over the past decade. Unlike their predecessors, these new leaders — and the teams they lead — are devoted solely to addressing issues of educational and instructional technology, tasked with keeping the technology our schools run on safe and functioning.

The demands placed on these leaders are unprecedented; the burden of responsibility is massive; and the threats are relentless. Some students may spend more than half of their time in a digital environment, engaging with multiple applications each day and building up extensive profiles online in the process. Every interaction with an application represents a piece of potentially sensitive data that schools need to protect. Every application and every device presents a potential point of entry for a cyberattack. And the stakes are incredibly high: A single data breach or ransomware attack can lead to the release of thousands of sensitive records, which may include both student and staff social security numbers. Cyberattacks like these can cost districts millions, if not billions, of dollars. The magnitude of these risks cannot be overstated.

District technology leaders are now expected to not only manage and maintain existing systems but also stay abreast of emerging technologies, all while navigating the complexities of cybersecurity threats and budgetary constraints. This has resulted in a situation where CTOs often find themselves in the unenviable position of having to say “no” to new initiatives, projects and systems — not because they don't want to support innovation, but because they don't have the time or resources to do so.

The challenge lies in finding a way to balance the need for progress with the practical realities of limited resources and competing priorities. Technology leaders are often problem-solvers who think in binary terms: A problem is either solved or it's not. This can lead to a tendency to view decisions about new technologies in a similar way: They are either adopted or rejected. This approach can be counterproductive, however, because it can stifle innovation and create an environment where new ideas are met with resistance rather than enthusiasm. Peer end users, like teachers and other staff members, may not be aware of the myriad challenges CTOs and their teams are facing. Instead, they only know that leaders have rejected their request to use their favorite app in the classroom or on campus. In their minds, the IT Department has become the “Department of No.”

But it doesn't have to be that way. District technology leaders — some of whom are spotlighted in this report — have taken steps to transform their offices from the "Department of No" into the "Department of Know" by navigating the many tensions CTOs face in context. A more effective approach to choosing new apps, for example, is to shift the focus from a binary yes-or-no decision to a more open-ended "how?" Instead of simply rejecting a new technology because it doesn't meet all the requirements, tech leaders can explore ways to make it work. This might involve finding creative solutions to technical challenges, negotiating with vendors to get a better deal, or reallocating resources to free up time for implementation.

By adopting a "how" mindset, technology leaders can foster a culture of innovation and collaboration, where they welcome and explore new ideas rather than dismissing them out of hand. They can build bridges and relationships with other leaders in the district, giving every department a window into the challenges that IT faces and a reason to buy in. This approach fosters trust and respect between technology leaders and other stakeholders, because it demonstrates a willingness to listen and find solutions that work for everyone.

Ultimately, the goal is not to say "yes" to every new technology or to avoid conflict at all costs. Rather, it's to negotiate a way through the complexities of the educational technology landscape in a way that supports innovation, promotes collaboration and ensures that all students can safely benefit. This requires a willingness to think creatively, to be open to new ideas and to work collaboratively with others to find solutions that meet all stakeholders' needs.

# Executive Summary

Look at any large school system's organizational chart, and you will likely see a senior, cabinet-level position — possibly a chief technology officer (CTOs) or a chief information officer (CIO) — in charge of technology. While the titles may differ, even smaller districts are now elevating individuals tasked with overseeing the technology that powers school systems to district leadership positions.

But this wasn't always the case. Not so long ago, these technology positions either didn't exist or were viewed as "fixers" whose responsibilities didn't extend beyond keeping the lights on and the systems running.

Over the past few decades, much has changed in the world, and today's schools — like most other modern institutions — run on technology. From instructional applications to communications systems and from data systems to systems that monitor heating, ventilation and air conditioning and security systems, technology is everywhere in school districts.

Consequently, tech leaders (whom we may also refer to as CTOs in this paper) now have an even more critical role to play, focusing equally (and perhaps more than any other single person in a district aside from the superintendent) on the school system's two vital goals: 1) keeping students and staff safe and 2) ensuring students learn.

For CTOs, cybersecurity and data privacy are at the heart of the focus on safety.

Schools — as well as the student data and, increasingly, the student digital identities housed within their systems — have become the No. 1 target for cyberattacks. As a result of these ever-evolving threats and their consequences, CTOs have become focused on defensive security measures, like limiting the number of applications that can access a district's cloud or network, to protect sensitive information and keep systems safe. This has led, in part, to the perception of many educators and administrators that the tech office is really the "Department of No."

Technology is also ubiquitous in schools, however. Students may spend more than half of their time in digital learning environments, which need to operate seamlessly and fluidly to be effective.  Defaulting to "no" in this context could stifle innovation or opportunities to introduce new systems and tools that will benefit teachers and students – or that teachers and students may already love. Indeed, this is why saying "no" too often may be counterproductive no matter how well-intentioned, because it can lead to "shadow edtech" in classrooms – tools that educators decide to use anyway that lead to more headaches and  security risks.

Through interviews with school system leaders from across the country, this paper explores how innovative CTOs are transitioning their departments from the "Department of No" to the "Department of Know" by taking steps like:

- Creating clear criteria for adopting new tools that balance security and classroom needs
- Establishing robust protocols for protecting student data and digital identities
- Building cultures of shared responsibility for cybersecurity across all stakeholders
- Moving from reactive problem-solving to proactive strategic planning
- Fostering meaningful collaboration between IT and other teams (instructional, facilities, etc.)

The paper highlights how leading school systems are reimagining the CTO role — from tactical operator to strategic partner — to address evolving security challenges while enabling innovative digital learning experiences. It uses identity management as a concrete example of this shift, showing how modern approaches to identity can help technology leaders say "yes" safely rather than defaulting to "no."
The goal of this paper is not to provide an exhaustive treatment of these complex topics but rather to contribute to the ongoing dialogue about the evolving role of technology leadership in K-12 education, particularly as it relates to cybersecurity, student identity protection and safe digital learning. Clever, a global identity platform for schools, commissioned this paper, and readers should consider this context as they evaluate the perspectives and recommendations presented. The views that the interviewed school system leaders expressed reflect their individual experiences and do not necessarily represent those of their school systems or the broader education technology sector.

# Contents

# About the Authors

## Evo Popoff

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 education technology and school and school system improvement efforts. Prior to joining the department, he led the development of education technology 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

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 pre-medical studies. At the intersection of education technology, 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. More than 75% of U.S. K-12 schools use Clever to power secure digital learning experiences. And with Clever's layered security solutions, K-12 schools can protect school system 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.

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.

# Acknowledgements

*We're grateful to the education leaders who helped inform our perspective and contributed their insights to this paper:*

**David Boxer**

Chief Technology Officer,
The Blake School

**David Shulkin**

Director of Learning/Information
Technology, Bloomfield Hills Schools

**Eric Hileman**

Exec. Director of Information Technology,
Oklahoma City Public Schools

**Eric Krugler**

Chief Technology Officer,
Clever

**Eva Rodriguez Mendoza**

Chief Information Technology Officer,
San Antonio Independent School District

**Ji Soo Song**

Director of Projects & Initiatives,
SETDA, Former Advisor at the Office of
Educational Technology, U.S. Department
of Education

**Joe Phillips**

Chief Information Officer,
Fulton County Public Schools

**John Kraman**

Chief Information Officer,
Mississippi Department of Education

**Julia Fallon**

Executive Director,
SETDA

**Keith Krueger**

Chief Executive Officer,
CoSN

**Mark Racine**

Former Chief Technology Officer,
Boston Public Schools

**Rashad Slade**

Chief Information Officer,
Guilford Public Schools

**Thomas C. Murray**

Director of Innovation,
Future Ready Schools

# Introduction

Ask educators and administrators about the technology department in their school system and you may hear a reference to the "Department of No," as in:

"No, you can't use that application in the classroom."

"No, we don't support that tool in our school system."

For many educators and administrators, statements like these may sum up their experience with the school system's technology office. It's the "Department of No": The place that tells them they can't use the tools that they love and want to use with their students.

And this perception exists for a reason. The technology department does often say no — but open a newspaper, and you will see why these technology leaders need to be cautious.

K-12 school systems face an unprecedented security challenge: They've become the No. 1 target for ransomware attacks while operating with minimal security resources. In fact, school systems across the U.S. have demonstrated overwhelming demand for Federal Communications Commission E-rate cybersecurity funding, with $3.7 billion in requests dwarfing the allocation of only $200 million — despite strong interest in implementing security upgrades like advanced firewalls. To paint a bleaker picture, a recent survey found that more than half of school systems (53%) report insufficient cybersecurity spending, and satisfaction with current spending levels has dropped significantly — only 31% of administrators believe they're spending the right amount on cybersecurity, down from 41% in 2023. This has created a perfect storm where school systems must protect an incredibly complex ecosystem of users — from 5-year-olds to adult staff — with legacy systems that weren't designed for today's threat landscape.

The challenge extends beyond protecting data to safeguarding student digital identities, a concept that many school systems are just beginning to grapple with. In K-12 education, a "digital identity" is the collection of online credentials and data that represent an individual within a school system. For today's students, these digital footprints encompass everything from login accounts, passwords and app permissions to personal information (name, age, contact details), academic records, services they have received and behavioral patterns. On Dec. 28, 2024, for example, PowerSchool — the first of what will likely be many major edtech platforms to face such an attack — was hacked, exposing both students' and staff members' sensitive personal information, including social security numbers. This breach affected numerous school systems across the United States, and PowerSchool's products support more than 50 million students throughout North America. Digital identities are critical to support learning; but, if compromised, they can unlock access to sensitive information.

And while school systems now manage a complex ecosystem of 2,739 distinct edtech tools annually, only about one-quarter of school administrators are confident that they can protect students' identifying information. Students spend upward of 50% of their time in digital environments, and the traditional defensive security measures are no longer enough. A reactive stance, while well-intentioned, often leads to even greater security risks.

Just as students' relationship with digital learning has changed, so, too, has the role of the chief technology officer (CTO). The CTO position, often a cabinet-level position dedicated to technology alone, is now more common than ever, but current leaders may be the first in their school systems to have held the title.

CTOs must be centered on strategic technology leadership, which will require fundamental cultural shifts within school systems. Technology departments have historically operated in isolation, but modern challenges require collaborating across departments. Technology leaders must also be proactive about threat prevention, rather than reactive about threats as they occur and evolve from the "Department of No" into the "Department of Know" — by finding ways to enable safe digital learning rather than simply restricting access. At the same time, other cabinet-level leaders must embrace the CTO (or technology leadership in general) as a strategic partner in achieving educational goals — not just as a service provider to call when systems break.

As the CTO's role develops and evolves amidst growing cyber threats to K-12 systems, we are faced with a unique — or rather, imperative — opportunity for education tech leaders to learn from each other as they wrestle with a new generation of tech challenges.

This paper explores the current state of play when it comes to the security landscape of tech in schools as well as the accompanying tensions leaders are addressing. These tensions are many: supporting student learning while protecting student identities, keeping up-to-date with new cloud and edtech solutions while preventing cybersecurity incidents, and implementing artificial intelligence (AI) technologies in the classroom while remaining cognizant of the risks posed by these AI applications.

Through interviews with school system leaders from across the country, we explore how innovative CTOs are addressing these challenges by building cross-functional partnerships and developing frameworks for evaluating new edtech solutions as well as the steps leaders are taking to transition away from being the "Department of No" to being the "Department of Know" by creating clear criteria for adopting new tools, establishing protocols for protecting student data and identities, and building cultures of shared responsibility for cybersecurity.

# State of Play: Why Traditional Approaches No Longer Work

## Our New Security Landscape

The K-12 system is uniquely vulnerable to cyberattacks for many reasons, including users from a wide range of backgrounds with differing experiences of technology, high student and staff turnover, and limited budgets to bring everyone up to speed. Few other major organizations have to deal with adult professionals as well as very young users (who may not yet know how to read or type) and their parents, whose backgrounds vary widely — all while under immense budget constraints.

The cybersecurity challenges facing K-12 schools are daunting, with limited resources to address growing threats. John Kraman, Chief Information Officer, of the Mississippi Department of Education, emphasizes the urgent need for a more unified approach: "On the security front, school districts struggle with limited funding, skill and staffing shortages, and insufficient awareness. They are isolated on an island, fighting alone. A consolidated strategy is crucial to prevent isolation and enhance defenses against constant cyber threats."

Firewalls — a common solution implemented in school systems — alone aren't enough in a cloud-first digital world. While firewalls can block dangerous intrusions into a school system's local network or set conditions for certain kinds of outgoing traffic, they cannot prevent cloud-based hacks or attacks that might come through students' own accounts, laptops or cellphones. Depending on the kind of application in play, a hack might even find its way in through an account belonging to a student's parent or guardian.

On top of these challenges, school systems must also deal with legacy systems and applications, many of which do not address current issues relating to cybersecurity and data theft. "We have transitioned away from many of our legacy systems that were developed decades ago. When I transitioned to Technology Services, there was no documentation as to how databases were connected to critical operations, and the original developers were long gone. We have since updated our servers and security protocols, while moving toward a modernized enterprise management system to replace legacy systems," Rashad Slade, CTO of Guilford County Schools, says. "It's like trying to update the engine of a plane while it's flying."

## What Happens When Security Fails: Real-World Examples and Impacts

The consequences of cybersecurity breaches in K-12 education are severe and far-reaching, and compromised student identities can lead to long-term consequences potentially affecting students' future financial, educational and employment opportunities. Educational institutions faced 116 confirmed attacks in 2024, impacting 1.8 million records with the average ransom demanded hovering around $847,000. And in 2023, schools lost an average of 12.6 school days to ransomware attacks, with the average cost of downtime estimated at $548,185 per day. But these statistics only tell part of the story — the real impact is felt in classrooms and communities across the country.

This past fall 2024, Highline Public Schools in Washington State demonstrated just how disruptive these attacks can be. A ransomware attack forced the closure of 34 schools serving 17,500 students, canceling classes for multiple days at the start of the school year. The school system had to reimage thousands of devices, highlighting how a single security incident can bring learning to a halt.

Even more concerning are attacks targeting student data and student identities. In 2022, the Los Angeles Unified School District (LAUSD) experienced one of the most significant breaches when the ransomware group Vice Society infiltrated the district's network using leaked virtual private network (VPN) credentials. The attackers stole 500 gigabytes of sensitive data, including student records, Social Security numbers, driver's licenses, historical academic records and contractor payroll information. When LAUSD refused to pay the ransom, the group leaked the stolen information on the dark web — demonstrating how these attacks can have long-lasting consequences for students and staff long after systems are restored.

These high-profile attacks highlight a fundamental shift in the cybersecurity landscape: As schools have become increasingly digital, attackers have evolved their strategies from targeting school systems to targeting student identities themselves. This transition requires school systems to fundamentally rethink their approach to security.

## The Rise of AI: A New Security Challenge

While school systems work to defend against traditional security threats like ransomware and data breaches, the landscape is rapidly evolving, and emerging technologies are creating entirely new security challenges.

AI, in particular, has created a critical new battleground in cybersecurity, and AI presents challenges that are both novel and extreme. While 70% of administrators believe AI is increasing cybersecurity risks, schools lack preparedness to manage this threat. Only 46% have any process for vetting AI in edtech products, and a mere 9% have formal procedures, highlighting a critical gap between recognized risk and practical oversight.

> "You've got to be careful of who owns AI...District technology staff are just the gatekeepers but you've got to work with the instructional side to understand how to use it, why to use it, and what goals you're trying to achieve in the classroom."
>
> **Rashad Slade**
> Chief Information Officer,
> Guilford Public Schools

School systems face mounting pressure to adopt AI-enabled edtech tools — often from their own staff — and as a result, many are introducing AI applications into the classroom before establishing operational foundations and guidance for educators, creating unnecessary risks and complexity. "A lot of school systems want to dive right into the hardest part: classroom AI," Krueger says. "But finding early successes in more mundane areas, like central operations, can save money and time while building trust."

When it comes to the classroom, Krueger notes, "Our role is to educate teachers on how to use these tools the right way. But you have to start with getting your team using AI tools in a safe environment, preferably on things that only affect administrative work." Technology leaders must guide their school systems toward a more strategic approach, starting with administrative efficiencies and clear policies before moving to student-facing applications. SETDA and its partners in the EdTech Quality Collaborative have developed procurement guidance to help school systems evaluate AI and other edtech tools against key indicators, including safety, evidence, inclusivity, usability and interoperability, providing a framework for this careful balance between enabling innovation and ensuring responsible implementation – particularly given the unique privacy and security considerations in K-12 environments. "As districts race to adopt AI tools, we need a strategic approach to procurement that prioritizes both effective instruction and responsibility," says Julia Fallon, Executive Director of SETDA. "By evaluating tools thoughtfully against established criteria, school systems can make informed decisions that amplify teaching and learning while safeguarding student privacy and data."

## From Digital Access to Digital Identity

Today's K-12 students exist in two worlds simultaneously — physical and digital. Students may spend more than half of their school day in online environments, generating extensive digital footprints that encompass not just basic personal information but detailed portraits of their academic performance, behavioral patterns and learning preferences. The arrival of AI and other sophisticated threats makes protecting these digital identities even more critical, because malicious actors have new tools to potentially exploit this wealth of student data.

This digital trail is increasingly valuable: According to the U.S. Department of Education, a single stolen student record now sells for up to $300 on the dark web — significantly more than most other types of personal data. And the stakes are higher than ever, because what's at risk isn't just a username and password — it's a student's entire digital identity. "School systems often focus on protecting staff accounts, but student identities are increasingly valuable targets," explains Eric Hileman, Executive Director of Information Technology of Oklahoma City Public Schools. "Bad actors know this and are actively exploiting this gap in our security thinking."

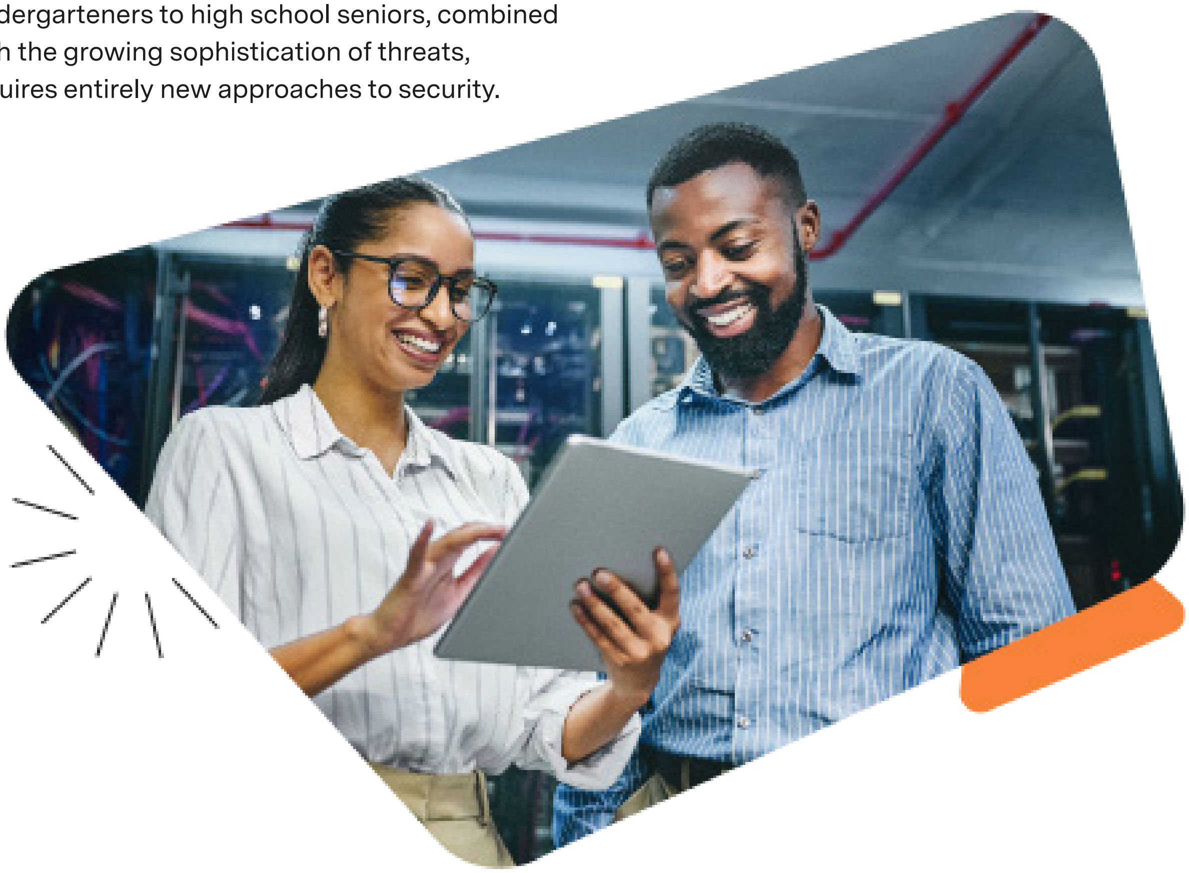
This evolving threat landscape requires a fundamental shift in how school systems approach security. While traditional account security is typically focused on preventing unauthorized access to specific systems, protecting digital identities requires safeguarding the entirety of a student's digital presence: their personal information, learning data, online interactions and digital access rights across multiple platforms.

What makes this challenge particularly acute is that digital identities aren't optional in the modern K-12 system. "School systems have to understand that digital identity is now fundamental to education," Hileman emphasizes. "Our systems run on technology and it's impossible to avoid creating robust student digital footprints. So we have to focus both on creating seamless access for students and security at the same time."

While school systems have made significant strides in securing staff accounts — with multi factor authentication (MFA) adoption rising from 42% to over 70% of school systems in just two years — protecting student identities is a unique problem. For students, it's not just about securing accounts, because those accounts protect an entire digital identity. "Implementing these protections for students, especially younger ones, presents a whole different challenge," notes Krueger. The wide age range of users, from kindergarteners to high school seniors, combined with the growing sophistication of threats, requires entirely new approaches to security.

The situation is further complicated by a growing trend toward banning cellphones in schools. This means school systems have to develop new and innovative workarounds for safeguards like MFA, which typically require a second personal device (like a cellphone) for authentication.

These mounting challenges around student digital identity protection exemplify why the role of technology leadership in K-12 education has had to evolve fundamentally. As threats become more sophisticated and the stakes continue to rise, school systems need strategic technology leaders who can balance security with educational access — not just technical experts focused solely on managing systems. This evolution of the technology leader's role from tactical operator to strategic partner has been gradual but transformative, reshaping how school systems approach both security and innovation.



# Reimagining the CTO Role: The Strategic Technology Leader

## A Brief History

The role of a CTO in K-12 school systems is still relatively new, having developed in earnest only over the past decade. As Keith Krueger, CEO of the Consortium for School Networking (CoSN) explains, when school systems first introduced the CTO title about 20 years ago, "it was a job description before there were people in that sort of position," defining what strategic technology leadership should look like at a time when most school systems only had technical coordinators. But as the uses of technology in education have increased, the threats posed by those technologies have grown as well — meaning more school systems are creating senior tech leadership roles that, not so long ago, didn't exist. This history, in part, explains why, to this day, many school systems struggle to position technology leadership appropriately.

This evolution mirrors what happened in school finance decades ago, says Krueger: "The most parallel universe was with finance probably 40 to 50 years ago. You know, there were bookkeepers and accountants. Almost every school system has a chief financial officer now, because it's a strategic asset."

Today's CTOs are similarly shifting from purely technical roles to strategic partners in their school systems' broader missions, although this transition remains a work in progress in many places. And this evolution requires balancing day-to-day operations with long-term strategic planning while building crucial relationships across departments.

The role's newness is evident in the varied backgrounds of those who hold it. According to CoSN, only about 40% of K-12 technology leaders come from IT backgrounds, with nearly 50% having education backgrounds instead. This diversity of experience can be an asset, because effective technology leadership requires understanding both the technical and educational sides of the role."The face of what a CTO is has changed. Increasingly, they're folks who need to understand instructional design and what is required to support teaching and learning " explains Thomas C. Murray, Director of Innovation for Future Ready Schools. "I was one of those folks—I was a school leader who became a district technology leader – and that background was incredibly valuable as I worked with the boxes and wires experts in my district to put in place the systems that advanced innovation while also meeting our broader technology needs."

CTOs who come from IT backgrounds need to develop a deep understanding of pedagogy, learning outcomes and classroom dynamics to make effective technology decisions. Conversely, those with educational backgrounds must quickly master complex technical concepts around cybersecurity, system architecture and emerging technologies like AI.

> "The most successful CTOs I've seen are those who can bridge both worlds...they can talk about security protocols with their IT team in the morning and then shift to discussing outcomes with curriculum directors in the afternoon. That versatility is crucial."
>
> **Eric Hileman**
> Exec. Director of Information Technology,
> Oklahoma City Public Schools

"The days of the CTO being just 'the tech person' are long gone," notes Hileman. "We're educational leaders who happen to specialize in technology, not the other way around."

## How the "Department of No" Emerged and Why It's a Difficult Mindset to Shift

Whereas IT departments in schools were once focused on edtech solutions and rejecting those applications deemed "unsafe" or restricting access to certain users, this "Department of No" mindset is no longer enough to manage the current tech landscape. Eva Rodriguez Mendoza, CTO of San Antonio Independent School District, explains: "It was definitely the 'Department of No' when I got here. It's a lot easier to maintain systems when you just get to say, 'No, we're just going to do Office, and we're not going to do Google. We're just going to support Apple products and not Apple and Dell.' But is that really what's best for our students?"

This tension is particularly acute in the classroom, where teachers increasingly rely on a growing number of digital tools to support student learning. Teachers are natural innovators, constantly seeking and discovering new tools and resources to enhance student engagement and learning outcomes. So, when IT departments consistently reject these tools without providing viable alternatives, security and pedagogical innovation are put at odds with one another. And such rejections can be counterproductive, because teachers may simply go around the tech office and use the tools they think best regardless of security guidelines, leading to "shadow edtech" in the classroom — and a higher risk of both logistical headaches for staff and potential hacks.

As such, the key challenge for modern IT departments is evolving beyond simple rejection to a more collaborative approach — working proactively with teachers to find and vet secure alternatives that meet their pedagogical needs while maintaining necessary security standards.
And such rejections can be counterproductive, because teachers may simply go around the tech office and use the tools they think best regardless of security guidelines, leading to "shadow edtech" in the classroom — and a higher risk of both logistical headaches for staff and potential hacks.

"You can't really make recommendations or be a thought partner if you don't understand their world," Rodriguez Mendoza says. "I have a safety and security division under IT with a lot of physical security — cameras, access control, intrusion alarms. It's not just keeping it up and running, but really the strategic vision around what it looks like to keep our schools safe."

Nevertheless, the persistence of the "Department of No" mindset stems from deep structural challenges that make it difficult for school IT departments to evolve, even when they recognize the need for change. At the most basic level, many school systems remain trapped in a reactive, break-fix cycle that consumes most of their IT team's time and energy. While departments want to be more proactive and strategic, they find themselves caught in an endless stream of immediate problems — fixing broken devices, responding to security alerts and troubleshooting network issues.

This reactive approach is exacerbated by severe resource constraints. With 53% of school systems reporting insufficient cybersecurity spending and satisfaction with current spending levels dropping significantly, many IT departments lack the basic resources needed to break out of this reactive cycle.

Staffing presents an equally challenging barrier. As Hileman notes, “In K-12 schools, you can’t pay people competitive wages if they have advanced technical skills. They’ll go to the private sector and make 3 to 4 times more. So we have to think differently about how we structure our technical operations.” This creates a vicious cycle where departments can’t retain the talent needed to build institutional knowledge and develop more sophisticated approaches.

The situation is poised to become even more challenging as Elementary and Secondary School Emergency Relief Fund funding ends. As Slade explains, “The pandemic pushed us into one-to-one computing, but now we have to figure out how to maintain it with no additional funding. You’re seeing decreasing enrollment but increasing technology needs. It’s a difficult balance.”

Meanwhile, the scope of IT responsibilities continues to expand exponentially. As Krueger observes, “The problem isn’t showing relevance anymore. Everything runs on the network. The problem is everything from security cameras to locks to HVAC ... What is it that the IT department should be in charge of?” This expanding mandate, combined with shrinking resources, makes it increasingly difficult for departments to shift from reactive problem-solving to proactive planning and innovation.

Breaking free from the “Department of No” mindset requires addressing these fundamental structural challenges. IT departments need adequate resources, stable staffing and clear scope definition to move beyond merely rejecting risky solutions and toward proactively developing secure alternatives that meet their school systems’ needs.

# Enabling vs. Restricting: A New Security Paradigm

Based on our interviews, CTOs identified several concrete steps that are critical for changing this paradigm. These include establishing clear evaluation processes and committees to assess new tools; creating "sandbox" environments where teachers can safely pilot new technologies; and most importantly, shifting their default response from "no" to "how can we make this work safely?" For example, while one district initially rejected consumer AI tools like Alexa due to privacy concerns, it later approved enterprise versions of similar tools that met their security requirements. As Dr. Joe Phillips, CIO of Fulton County Schools, explains, modern IT departments should "start with yes, arrive at no" — having clear criteria for when security concerns require rejection, but approaching each request with an intent to enable rather than restrict.

## Building a Cross-Functional Partnership

Collaborating across departments is critical, whether CTOs are preparing for the next big app or the next generation of leadership. As Murray emphasizes, "the importance of working together can't be overstated—different backgrounds bring different expertise. If we are restricting something, we need to explain why we're restricting it and offer alternatives that can still meet those instructional needs. That communication is huge."

Involving other stakeholders is critical, especially when it comes to instructional tools. To foster innovation on the instructional side, CTOs can involve teachers at all stages of the process, from creating evaluation committees to developing evaluation processes and from piloting a new application or tool to implementing it.

CTOs must orchestrate collaboration across curriculum, operations and administrative teams while managing onerous resource constraints — including staff turnover. In the words of Slade: "You can't create 'unicorns' – staff members who hold all the knowledge about critical systems. When they leave, you're in trouble. We have to build structures that allow for knowledge sharing and succession planning."

Instead of working in isolation, the IT department's role should be integrated into all departments it serves. David Shulkin, director of instructional technology at Bloomfield Schools, emphasizes this approach: "For technology leaders, what helps get that seat at the table is engaging the end user in a much more intimate way. It's building those relationships and having those conversations about what's really happening, what people are struggling with."

And to deal with increasing budget pressures, leaders will have to engage finance and operations teams. The IT department must also build relationships with school leaders. Together, leaders and school systems can move forward as a unified front to develop the best, and most secure, experience for students.

> "You have to create ongoing, consistent collaboration teams. Instead of just saying no, explain why something might not work right now and offer alernatives that could work in the meantime. It's about finding a path to yes, even if it's not immediate."
>
> **Rashad Slade**
> Chief Information Officer,
> Guilford Public Schools

## How to Say Yes (Safely)

School system technology leaders are developing frameworks to enable innovation — for example, by allowing the addition of new technologies, devices or apps to a school's network — while maintaining security through clear criteria and processes. "We've established a school system review committee with both technical and instructional contacts to evaluate new requests to adopt new edtech tools," Slade continues. "This allows us to systematically evaluate each proposal while keeping security and educational value in focus."

Thoughtfully evaluating requests and explaining how a decision was reached builds trust between departments and stakeholders, Rodriguez Mendoza adds: "The CTO today really needs to be able to build relationships and build trust within the district. I'm not the subject matter expert, but I'm giving recommendations based on technical specs or technical needs. Sometimes we do have to say no, but you don't say just no. You say, 'This doesn't work right now, and this is why. Let's find you a solution that does work with our network, that is secure, that is protecting our data.'"

Shulkin emphasizes a similar methodical approach: "We evaluate each request by looking at the core problem they're trying to solve, examining whether our existing solutions could meet that need, and then carefully considering the privacy and security implications." This systematic evaluation helps technology leaders move from defaulting to "no" toward finding secure paths to "yes." Murray shares a personal experience that illustrates how these collaborative evaluations work in practice: "When I joined, one of the technical staff was skeptical about my plans to improve access to a program I thought would make life easier for teachers. He showed me how opening up that access would impact our network bandwidth, leading to a valuable conversation about balancing convenience with technical constraints. Having both types of experience in the department enables these important conversations and helps us message our decisions effectively."

## Escaping the Break-Fix Cycle and Moving From Reactive to Proactive Leadership

CTOs aren't leading just to "fix" systems or applications that are "broken." CTOs are critical participants in achieving a district's vision for teaching and learning and for maintaining students' safety and security — perhaps the most important goals in a school system. Consequently, they need to be leading with a proactive mindset — not only anticipating threats but also understanding how decisions will impact instruction.

Phillips, of Fulton County Schools, emphasizes the importance of forward thinking: "Technology leaders need to position themselves 18 to 24 months ahead of the work coming down the pipeline. It's about anticipating needs rather than just responding to them." This proactive stance includes developing technology refresh cycles, establishing clear processes for evaluating new technologies and creating systematic approaches to scaling successful initiatives. The goal is to shift from constantly fighting fires to preventing them from starting in the first place.

The best leaders in this role will engage everyone in discussions and decisions around cybersecurity before attacks, intrusions and bad actors become a problem. As Phillips explains, “I realized we needed to shift from being reactive to proactive. Instead of waiting for problems, I started meeting with department heads to understand their goals and position IT as a strategic partner in achieving them.” This proactive approach represents a key distinction between technical coordination and true technology leadership.

## Building Cybersecurity Awareness Across the School Community

Cybersecurity doesn’t begin and end with teachers using applications in the classroom. Parents and students, as well as staff at all levels, need to understand the grave consequences of a threat intrusion — and how they can prevent an intrusion from happening.

“Technical solutions alone aren’t enough — the human factor remains our greatest vulnerability,” notes David Boxer, CIO of The Blake School. “We could invest millions in cybersecurity infrastructure, but without educating our users, we’re missing the critical piece.”

Successful school systems are implementing comprehensive awareness programs that combine regular training, simulated security exercises and clear incident reporting protocols. This includes integrating digital citizenship into curriculum and engaging parents in security awareness — recognizing that cybersecurity is a shared responsibility that extends beyond school walls.

## Engaging Stakeholders in Security Decisions

Unilateral decisions won’t work, and school systems must follow building awareness with getting buy-in. Everyone who has a role to play in the school system, from parents and students to facilities and front office staff members, has a role to play in keeping schools secure, and they need to know that their voice matters.

Effective security requires investment and participation from all stakeholders.

> “Success comes from understanding everyone’s road map and finding ways to align them...When we engage stakeholders early and often, we can develop solutions that work for everyone.”
>
> **Joe Phillips**
> Chief Information Officer,
> Fulton County Public Schools

This means regular engagement with department heads and transparent decision-making processes. The most successful school systems have found ways to make security everyone’s responsibility while ensuring all voices are heard in the process.

# Recommendations and Next Steps

The evolution of technology leadership in K-12 schools presents both an unprecedented challenge and an extraordinary opportunity. As school systems navigate an increasingly complex digital landscape, the transformation from tactical tech management to strategic leadership becomes not just desirable but essential for safeguarding school communities.

The path forward requires embracing a new paradigm where technology leaders serve as strategic partners rather than just service providers. This means moving beyond the perceived "Department of No" mentality and building collaborative frameworks that enable innovation while maintaining security. Success comes not from having all the technical answers but from building relationships across departments, understanding the varying needs of different user types, and creating systems that support both security and innovation.

The stakes are particularly high given the changing nature of what needs protecting. As students spend more time in digital environments, technology leaders must expand their focus beyond traditional network security to safeguard students' entire digital identities. This requires new approaches to security that consider classrooms' unique challenges — from protecting very young users to managing complex ecosystems of tools, applications, and student and staff data.

The opportunity (and imperative) for technology leaders has never been clearer: As the threats continue to evolve and the importance of digital learning grows, technology leadership must evolve and grow as well. The future belongs to leaders who can balance innovation with security, tactical needs with strategic vision and technical expertise with educational understanding. The transformation from "no" to "know" represents more than just a change in approach — it represents the future of edtech leadership.