The Leadership Imperatives for K-12 Cybersecurity in the Age of AI

2025 iboss-Project Tomorrow National Research on K-12 Cybersecurity

The Leadership Imperatives for K-12 Cybersecurity in the Age of AI

Key findings from the 2025 iboss-Project Tomorrow National Research on K-12 Cybersecurity

"Cybersecurity is not just a technical concern—it is a leadership priority. In today's digital landscape, district leaders must move beyond reactive measures and establish long-term cybersecurity strategies. This includes leveraging emerging technologies like AI, fostering district collaboration, and driving policy changes at the state and national levels."[i]

Tom Ryan and Lenny Schad
Former CIO's and Co-Founders K12 Strategic Technology Advisory Group

Introduction

In this highly dynamic education environment, today's K-12 technology leaders need be both nimble and adaptive. Nimble to address changing expectations from leadership and stakeholders about the role of traditional technologies within learning (i.e., online curriculum, student devices, social media); adaptive to understanding how to effectively evaluate and implement emerging technologies to better meet their district vision for learning in 2025 and beyond (i.e., Generative AI, immersive technologies, robotics). In both contexts, cybersecurity and in particular data protection and privacy continue to be critical issues within schools and districts today.

Central to this reality is an increasing tension for K-12 technology leaders: How to effectively leverage both traditional and emerging technologies to support student learning and future-ready skill development while at the same time being strategic and forward thinking about what is required to protect district infrastructure and digital assets from nefarious actors with bad intentions. As noted in the quote from Tom Ryan and Lenny Schad, both former K-12 district Chief Information Officers, the solution is this tension is not a quick technical fix or new product implementation. Rather, what is needed today is a new type of K-12 technology leadership that understands both the technical and human sides of today's digital landscape.

Since 2017, Project Tomorrow® has been collecting and sharing the views of K-12 leaders about cybersecurity issues through our annual Speak Up® Research Project. For the past six years, we have collaborated with iboss on a highly targeted study that examines the state of K-12 cybersecurity awareness and preparation in our nation's school districts from the perspective of technology leadership. The findings from this research regularly inform the policies and initiatives of K-12 school districts nationwide. Our nation's K-12 CIOs and CTOs understand what is at stake today with cybersecurity. According to the latest Project Tomorrow research, two-thirds of K-12 district leaders (67%) say that addressing cyber threats and protecting district assets is their number 1 most challenging issue today. District leaders (55%) identify establishing and enforcing Generative AI policies and guidelines as their second most important challenge. These top two challenges are inevitably linked. When asked about current risks for a cyberattack, 88% of district leaders said they believe that K-12 schools and districts are at a higher risk today than ever before. The potential use of AI within cyber-attacks is often cited as the reason for that increased risk today.

Given that context, our focus in this year's state of cybersecurity report is on both understanding what has changed in K-12 cybersecurity over the past few years as well as reflecting on the potential impact of Artificial Intelligence (AI) as it relates to cybersecurity. Both views are important to understand the current context for cybersecurity leadership in our K-12 districts. Using feedback from 2,310 district technology leaders representing a diverse set of K-12 districts nationwide, this year's report, *The Leadership Imperatives for K-12 Cybersecurity in the Age of AI,* continues our legacy of supporting district technology leaders in their important work to ensure that the data, infrastructure and resources within their networks are protected. Additionally, this year we have used the research findings to identify five (5) key cybersecurity realities that are driving the need for enhanced leadership and a new prioritization of cybersecurity in K-12 institutions. Within each of the five realities, we are positioning a new leadership imperative in the form of a question for consideration by K-12 district technology leaders as they navigate the choppy waters of cybersecurity in the age of AI.

The five (5) key cybersecurity realities that can help usher in these new leadership imperatives around cybersecurity in K-12 education are the following:

1. Greater awareness of cybersecurity implications drives an increased sense of urgency to protect district assets and infrastructure.

2. Explaining the value proposition of effective cybersecurity preparations is more effective when the message is in the same language as the receiving audience.

3. While K-12 education's approach to challenges is often to address the symptoms that mask the real causes, cybersecurity today demands a root cause analysis to create more successful strategies for asset protection.

4. Effective cybersecurity preparation and response require a districtwide ecosystem approach.

5. Embracing AI as both an opportunity and a threat in K-12 education unlocks new discussions about effective cybersecurity.

Each of these realities represents a chapter in this year's report. To support ongoing discussions, we have identified key research data that supports the premise of each reality and its relationship to the identified new leadership imperative. Our goal with this year's report is to have it be actionable and supportive of your local efforts to continuously improve your district practices around cybersecurity. But these efforts do not need to take place in isolation. We are here to help you. For more information about how to use this report within your district or how Project Tomorrow can support your district's leadership on cybersecurity in the age of AI, please contact us at innovation@tomorrow.org.

Cybersecurity Realities and the New Leadership Imperatives

Reality #1: Greater awareness of cybersecurity implications drives an increased sense of urgency to protect district assets and infrastructure.

New Leadership Imperative: What can you do to create a wider circle of cybersecurity awareness within your district?

Nearly two-thirds of district technology leaders (65%) say they are more concerned today about a cyber-attack or incident in their district that a year ago. These leaders attribute their increased concerns about a cybersecurity incident to several factors (Table 1). Topping their list of factors is familiarity with a district in their state or region that has had a cyberattack (60%). Other contributing factors include increased national reporting on cyber incidents in K-12 schools and districts (52%) and a clearer understanding about the potentially dangerous role that AI can play in new threat strategies (47%).

Table 1: Why are you more concerned about a cyberattack in your district today?

Factors contributing to higher cyberattack concern	% of technology leaders
Knowing a district that has had a cyber attack	57%
National reporting on increases in attacks within K-12 schools and districts	52%
Understanding the potential role of AI in cyberattack strategies	47%
Understanding the potential impact of an attack on learning disruption	42%
Local reporting on companies and organizations in our area who have had a cyberattack	33%

District leaders are increasingly concerned about a wide variety of types of cyberattacks in their districts. Of high concern are data breaches that involve the sharing of the personal information of staff (cited by 70% of district technology leaders) and district students (cited by 62% of district technology leaders). Technology leaders continue to be also concerned about phishing scams (67%), ransomware attacks (66%), business email compromise (BEC) type scams (58%) and data breaches that result in the loss of financial information (52%).

The increased emphasis on data privacy and protection especially for students is in alignment with parents' concerns as well. When parents and families were asked about their concerns about the potential role of AI in education, 64% of parents say their top concern is around how their local schools are adequately storing and protecting their children's data.

Per other Project Tomorrow research reporting, district leaders are particularly interested in parent perception of local schools. Therefore, school districts may be reluctant to publicly announce a cyber data breach specifically to avoid reputational fallout or to lose the trust of parents.[ii] Another reason may be because districts are concerned that their internal training programs around cybersecurity may not be highly effective as desired or required to protect student data.

While 54% of district technology leaders say their cybersecurity training for their technology staff is highly effective, only 15% say the same about training for their classroom teachers (Table 2).

Table 2: How effective are your current cybersecurity training programs within your district?

Training audience	% of technology leaders	
	Our training is highly effective	Our training is somewhat effective
Technology staff	54%	40%
District executive leadership	24%	55%
District curriculum and learning services leadership	17%	60%
School principals	17%	61%
Teachers	15%	57%
Students	8%	34%

As noted in Table 1, 42% of district technology leaders noted that their increased concern about cyber threats is being fueled by a new understanding of the potential impact of an attack on learning disruption. This is a real concern. According to reporting from a 2022 U.S. Government Accountability Office report, a cyberattack can result in learning time loss of three days to three weeks.[iii] This reality can be a new driver for improving the effectiveness of cybersecurity training across all audiences. With more effective training programs in place, district stakeholders may develop a stronger awareness about the risks of a cyberattack and be more responsive to the policies and strategies enacted by the technology department to protect district assets. This can help the district technology leadership raise the stakes on the urgency around cybersecurity within their district.

Reality #2: Explaining the value proposition of effective cybersecurity preparations is more effective when the message is in the same language as the receiving audience.

New Leadership Imperative: How effectively can you translate the technical language of cybersecurity so that it more clearly resonates as a leadership priority in your district?

One of the most common refrains we hear from district technology leaders is their frustration that their colleagues in the district office or Cabinet are not sufficiently aware or concerned about cybersecurity and the potential risks to the district of a cyberattack. This lack of general awareness impacts the district technology leaders' abilities to have cybersecurity prioritized as a high need within their district.

To understand the prioritization of cybersecurity within K-12 districts, district technology leaders were asked to agree or disagree with this statement: *Our district has made the establishment of cybersecurity policies and procedures a high-level priority for this year.*

District Technology Leaders' responses:

- 22% strongly agree
- 39% somewhat agree
- 39% either disagree or are not sure

While 61% in total say that cybersecurity is a high priority in their district, that support is tepid, with only 22% strongly agreeing with that proposition. As noted above, this lack of strong leadership prioritization may be a result of a lack of awareness or concern about the multitudes of risks of cybersecurity in a district. In general, district technology leaders say that their colleagues do not have elevated levels of awareness today about the need for cybersecurity with one notable exception (Table 3).

Table 3: How would you rate the awareness level of your colleagues on your district's risk or potential vulnerability to cyberattacks?

Categories of district colleagues	% of technology leaders		
	High level of awareness	Moderate level of awareness	Low level of awareness
Chief Business Officer/Chief Financial Officer	47%	44%	9%
Superintendent	39%	49%	13%
Cabinet (as a group)	27%	57%	16%
Communication/PR Officer	26%	52%	22%
School Board	18%	49%	32%

The exception to the general findings is the awareness level of the Chief Business Officer or Chief Financial Officer. Notably, 47% of district technology leaders say that their CBO or CFO's level of awareness is at a high level today. This represents an increase of 10 percentage points compared to their answer to the same question in 2022. The awareness levels of the other district colleagues have not changed substantively, however, since 2022.

We believe that the increased focus on procuring cybersecurity insurance over the past few years has led to this greater awareness by CBOs and CFOs about the financial risks to their district of a cyber incident. Two-thirds of district technology leaders (66%) now identify that their district has an insurance policy as part of their steps taken to reduce or mitigate cyber vulnerability (Table 4). In our 2022 reporting, only 23% of district technology leaders said their district had an insurance policy. CBOs and CFOs have definitely played a role in the procurement of those insurance policies and thus have had a front-row seat in discussions about the risks associated with a cyber-attack in ways they may not have before.

Table 4: What steps have you taken to reduce your district's vulnerability to cyberattacks?

Steps taken	% of technology leaders	
	This is in place now	We are working toward this
Secured an insurance policy	66%	16%
Require two-factor authentication for district accounts	62%	23%
Purchased specific cybersecurity products and services	54%	24%
Conduct annual security audit	46%	33%
Limit access to sensitive data by tightening admin privileges	46%	38%
Provide end-user training on a regular basis	46%	31%
Implemented a password change schedule district wide	44%	24%
Have an incident response plan in place	43%	38%

The following practices also saw significant adoption increases from 2022 to 2025:

- Limit access to sensitive data by tightening admin privileges: 35% increase
- Implement a password change schedule district wide: 42% increase

Given the example of how CBOs and CFOs are more responsive and aware of cybersecurity concerns because of their involvement with the financial aspects of cybersecurity, the idea of "speaking the language" of the district colleagues may be a good recipe to elevating their knowledge, awareness and concerns about the risks faced by the district.

This translation process may start with explaining the potential negative impact of a cyber incident. The district technology leaders identified the following as the most consequential negative impacts of a cyber-attack:

- Administrative operations disruption – 62%
- Learning disruption with loss of learning time or missed school – 54%
- Network disruption which impacted all departments – 51%
- Negative district PR with loss of trust and reputation in the community, especially with parents – 43%
- Financial impacts due to the need to potentially pay a ransom or to recoup lost data – 42%

Each of these results could have high resonance with a different set of colleagues in the district. For example, an explanation that a cyberattack may result in closing schools and the loss of learning time for students may be more compelling to a Chief Academic Officer than simply talking about an inoperable network or hacked email. For a district Communication Officer with responsibility for the district's public reputation, negative district PR because of a cyberattack could directly impact their ability to build local community support for a bond measure for example.

Audience specific messaging matters, especially in terms of driving greater awareness about cybersecurity. To help district technology leaders translate a technology message into an audience responsive message about district risks and vulnerabilities, Project Tomorrow in conjunction with the K-12 National Advisory Council on Cybersecurity released *"The Roadmap to Developing A K-12 Districtwide Cybersecurity Ecosystem – An Action Guide for Building Cabinet Buy-in."* This Action Guide is available here: NACC Cybersecurity Action Guide.pdf

Reality #3: While K-12 education's approach to challenges is often to address the symptoms that mask the real causes, cybersecurity today demands a root cause analysis to create more effective strategies for asset protection.

New Leadership Imperative: How will you lead the shift in your district away from fixing symptoms to understanding the root causes for why cybersecurity policies and procedures are so difficult to adopt and implement?

There is significant value in education in the discernment of symptoms and root causes. Understanding the root causes of a problem or challenge helps to identify and potentially fix underlying institutional conditions that may be blocking progress, not just treating the outward symptoms or representations of those issues. It is also possible with root cause analysis to avoid the recurrence of the same problems and a healthy way to position continuous improvement within an organization. Too often, cybersecurity solutions adopted by school districts are used to address symptoms, but not to directly get to the heart of an institutional problem or challenge affecting a district's cybersecurity posture. Given the ever-increasing risks and vulnerabilities in K-12 education for devastating cyber incidents, including those fueled by AI, it is time for us to think beyond quick technical fixes and address foundational challenges with K-12 cybersecurity.

District technology leaders identified both symptoms and root causes when asked to name the obstacles that inhibit their ability to effectively protect district networks as well as students, teachers and staff. For example, while lack of budget is a significant obstacle it may be most likely the result of district leadership's lack of awareness or understanding of the risks and vulnerabilities of not having advanced cybersecurity infrastructure. (Table 5). In that case, the lack of budget is the symptom; the lack of leadership knowledge or buy-in is the root cause. Given that general lack of awareness of district leadership about cybersecurity (Table 3) it makes sense that we continue to see districts that are not prioritizing cybersecurity or dedicating financial resources to support appropriate preparations. From this year's findings, only 43% of district technology leaders said they have a line item in their district budget for cybersecurity, and 41% noted that they do not.

Other key obstacles should also be evaluated as to whether they are a symptom or a root cause. Students and teachers circumventing existing cybersecurity practices is probably a symptom with a root cause being ineffective training. A reactive internal culture however may be the root cause for the lack of a strategic direction for cybersecurity adoptions. The opportunity exists for today's district technology leadership to provide direction on how to evaluate and mitigate the various obstacles that are preventing cybersecurity efficacy in the district.

Table 5: What are the primary obstacles you face in providing effective cybersecurity protections in your district?

Obstacles to cybersecurity efficacy	% of technology leaders	
	2022	2025
Balancing access to educational resources with security	45%	63%
Students and teachers circumventing existing policies	22%	49%
Lack of budget to invest in advanced infrastructure	36%	48%
Lack of technology expertise among teachers and administrators	33%	45%
Internal culture that is more reactive than proactive regarding security	34%	45%
Keeping up with the pace of technology adoption	33%	43%
School and district leadership do not understand the potential of cyberattacks	27%	42%

Reflecting again the increased sense of urgency by district technology leaders about cybersecurity, significantly more district technology leaders identified these obstacles are barriers in 2025 than in 2022.

Reality #4: Effective cybersecurity preparation and response require a districtwide ecosystem approach.

New Leadership Imperative: What do you need to drive greater prioritization for a districtwide ecosystem for cybersecurity?

In the shorthand of many district operations, anything having to do with digital tools or resources, from installing phone systems to the migration to cloud-based apps has been the purview of the technology department. But provisioning Chromebooks to students is very different than securing the district's network infrastructure and protecting data assets from a cyber-attack. And while the technical expertise for cybersecurity may reside within the technology department, the success of the implementation of protective measures depends upon buy-in across the entire organization from the executive leadership in the district office to the classroom volunteer. Cybersecurity requires a different mindset today, especially in the age of AI.

In our past reporting on the state of cybersecurity in K-12 education we have documented the conundrum of who "owns" cybersecurity in a district. In 2022, 67% of district technology leaders said that cybersecurity was still primarily an IT department responsibility, with little shared accountability across the district leadership team. That statistic fueled a call for the creation of a district ecosystem for cybersecurity where all stakeholders were invested in the preparation efforts, the practices put in place to protect the assets, and the ultimate success (or failure) of cybersecurity in the district.

In this year's reporting, we are seeing the beginning fruits of those efforts. Making progress toward the adoption of that district ecosystem of shared responsibility, only 56% of district technology leaders now say cybersecurity is owned primarily by the IT department, a decrease of 16% in the past three years. Despite this movement, more leadership buy-in is still required. This is evident when examining what district technology leaders say they need to be better prepared to thwart or address a cyberattack.

District technology leaders identify two types of needs for improved cybersecurity within their district. Internal factors such as leadership buy-in, greater funding, better trained staff and assessments to evaluate their own preparedness top the list (Table 6). External resources play an important role also and help to expand that ecosystem beyond district resources. Notable on that list is access to external experts, information about best practices and tools or solutions that can provide an external assessment of specific district risks. And twice as many district technology leaders say they need help providing professional learning for their district leadership on cybersecurity in 2025 (52%) as in 2022 (27%) reflecting that ongoing need to secure greater leadership awareness about cyber threats and why security measures are critical.

Table 6: What do you need to improve your cybersecurity posture in your district?

Needs to improve cybersecurity posture	% of technology leaders	
	2022	2025
Needs (internally focused)		
Increased funding for cybersecurity	39%	69%
Internal assessments we can use to evaluate our own readiness and preparation	42%	56%
More highly trained and experienced technology staff	33%	50%
Leadership buy-in on the importance of cybersecurity	42%	45%
Needs (from external resources)		
Experts to call on for advice	38%	55%
Professional learning for district leadership on cybersecurity	27%	53%
Education on best practices	49%	52%
External assessment of our district risks	24%	50%

This increased focus on looking for external resources to support their district ecosystem for cybersecurity is evident in other practices of the district technology leaders.

- 55% of district technology leaders say they are regularly monitoring national trends and information on cybersecurity now; only 32% were doing the same in 2022.
- District technology leaders are leaning on their membership associations (66%), their colleagues (60%) and conference participation (47%) to keep up on cybersecurity best practices.
- Vendor familiarity with the K-12 sector is more important than ever for district technology leaders evaluating cybersecurity solutions. Twice as many tech leaders say that is a must have for them today (64%) compared to what they said in 2022 (32%).

The deliberate and strategic inclusion of more external resources to support a district ecosystem for cybersecurity appears to be an emerging trend. We see this as a response not only to the increased threats of cyberattacks but the inherent complexities of cybersecurity in the age of AI.

Reality #5: Embracing AI as both an opportunity and a threat in K-12 education unlocks new discussions about effective cybersecurity.

New Leadership Imperative: How will your leadership role evolve to support cybersecurity in this age of AI?

The new discussions in K-12 districts about the role of Generative AI products and resources within education are resulting in an explosion of other new critical conversations that will ultimately have an impact on every aspect of teaching and learning. These new critical conversations include of course understanding data privacy and protection when using digital tools, but they also extend to topics such as defining digital literacy in the age of AI, redesigning assessments, preparing students with new skills, engineering new classroom instructional practices, and even evaluating the role of school as we know it today. And central to many of these discussions is the potential impact of AI on cybersecurity.

From our analysis of district technology leaders' perspectives on AI within their security operations, the prevailing point of view (53%) is that AI is both a threat and an opportunity relative to cybersecurity. This split screen perspective is similar to the 2024-25 Speak Up Research Project results from classroom teachers' opinion as to whether AI will negatively or positively impact K-12 education: 47% of classroom teachers say AI will negatively impact education and 53% say it will have a positive impact.[iv] We all have much more to learn about the potential of AI in the classroom and within cybersecurity.

District Technology Leaders: Is AI a Threat or an Opportunity for Cybersecurity?

- 53% say both
- 20% say opportunity
- 16% say threat
- 11% unsure

A sampling of the views of District Technology Leaders emphasizes this duality in the potential role of AI within cybersecurity:

"It is a mixed bag. We are using AI to monitor the network, find attackers attempting to compromise our network, log in with student accounts, etc. But the bad guys are using it at a quicker pace and a more efficient manner to create really convincing phishing messages and put together complex data from a variety of sources (dark web, data breaches) to convince users they are legitimate based on the information they provide. We are trying to educate users to not take unnecessary risks about opening files or emails that may be legitimate until they verify. It is an uphill climb."

Director of Technology (NY)

"We see AI as both an opportunity and a risk. It can help us detect threats faster and improve response times, which is valuable for a small team. But we're also aware attackers are using AI to create smarter phishing and automate attacks. Plans are to stay informed by CISA, MS-ISAC … Follow updates on AI trends and tools being used by both attackers and defenders. AI can strengthen our defenses—but we're preparing for both sides of it."

Director of Information Technology (CA)

"If the AI program is trained properly, AI will play a significant (if not the most important) role to identify and resolve cybersecurity issues. As technology progresses and the capabilities of those causing the attacks increase, human reactions will not be capable of intervening and thwart a cyber-attack without the use of AI. Over the past 6 months, products we renew or new programs we deploy are evaluated based on how well AI resources in the products perform."

Director of Technology (UT)

"I think AI can help with detecting and preventing low level cyber threats. However, with AI as a whole I feel that the ease of using AI to attack institutions may open the door for attackers that may not have previously had the skills to attack. Therefore, increasing the total overall attacks and the skill of the basic attacks. Also, the Higher end cybercrime organizations are going to invest and secure AI tools that may be more powerful than what a school district can afford to invest to protect themselves. Therefore, the net effect on AI for Schools to me will be a bad thing. The bad guys will ultimately have the money to have better AI than what the good guys can afford."

Chief Technology Officer (CA)

New ideas are emerging about how to leverage AI to support a district's cybersecurity goals. As noted in these quotes, those include using AI to support advanced threat detection, providing real-time threat intelligence, improving security operations, and creating more realistic and personalized training experiences for staff.[v] But the threat side of the equation is very real, also. Central is the ongoing concern about the protection of student and staff data. Depending upon the AI deployment in schools (sanctioned or shadow), the increased attack surface creates more opportunities for bad actors to take advantage of vulnerabilities. Additionally, AI is empowering more sophisticated attacks including with highly personalized voice and image fakes. All of this points to a significant leadership moment for our nation's schools and districts, and technology leadership.

Ending Thoughts

The following questions summarize what we have identified in this report as the New Leadership Imperatives for District Technology Leaders on Cybersecurity. These questions can be used for personal reflection, to inform strategic planning within your Technology Department or to support new district wide discussions about the role of cybersecurity in the age of AI.

- What can you do to create a wider circle of cybersecurity awareness within your district?
- How effectively can you translate the technical language of cybersecurity so that it more clearly resonates as a leadership priority in your district?
- How will you lead the shift in your district away from fixing symptoms to understand the root causes for why cybersecurity policies and procedures are so difficult to adopt and implement?
- What do you need to drive greater prioritization for a districtwide ecosystem for cybersecurity?
- How will your leadership role evolve to support cybersecurity in this age of AI?

For more information about how Project Tomorrow can support your district's leadership on cybersecurity in the age of AI, please contact us at innovation@tomorrow.org.

Appendix

About Project Tomorrow

Project Tomorrow's vision is to ensure that today's students are well prepared to be tomorrow's innovators, leaders, and engaged citizens. We believe that authentic learning experiences enable all students to develop the skills and mindsets needed for future success. Our work spans Efficacy Studies and Research that measure the real-world impact of educational innovations, the nationally recognized Speak Up Research Project that amplifies the authentic voices of millions of K–12 stakeholders, and New Learning Model Programs that support schools in designing future-ready teaching and learning. Since 2003, we have provided education leaders, teachers, and parents with research-based insights that drive data-informed decisions, improve student outcomes, and create more effective learning experiences for all. Learn more at www.tomorrow.org.

About the iboss-Project Tomorrow National Research on K-12 Cybersecurity

Project Tomorrow's Speak Up Research Project findings on the State of Cybersecurity in K - 12 education is a partnership effort with iboss. Respondents include 2,310 district leaders from a cross-section of academic, communication, executive, financial and technology departments in K - 12 districts nationwide surveyed from January through August 2025.

About iboss

iboss provides a Zero Trust SASE platform tailored for K-12 educational environments, focusing on student safety, cybersecurity, and compliance. It is a unified cloud-based solution that consolidates multiple security and management tools, such as web filtering (to ensure CIPA compliance), malware prevention, and Classroom Management. The platform allows schools to enforce consistent security policies across all devices—including Chromebooks, Windows, and macOS—whether students are learning on or off campus. Furthermore, iboss includes AI-powered student safety monitoring to detect risks like self-harm or bullying and offers a Parent Portal to give families visibility into their child's online activities. This integrated approach helps schools streamline IT operations, reduce costs, and maintain a secure and focused digital learning environment. Finally, iboss is E-Rate Eligible (specifically as Firewall-as-a-Service or FWaaS), which can help school districts secure significant federal funding, saving them considerable costs. Learn more about why iboss is considered a superior cybersecurity platform for K12: K12 Student Safety Monitoring & CIPA Compliance - iboss

---

[i] https://www.k12360.com/blog/the-future-of-cybersecurity-in-schools---ai-collaboration-and-leadership-3-of-3
[ii] https://www.the74million.org/article/kept-in-the-dark/
[iii] https://www.edweek.org/technology/schools-are-a-top-target-of-ransomware-attacks-and-its-getting-worse/2023/08#:~:text=The%20loss%20of%20learning%20time%20after%20a,2022%20U.S.%20Government%20Accountability%20Office%20report%20
[iv] 24-25 Speak Up Educator AI Infographic.pdf
[v] https://edtechmagazine.com/k12/article/2025/03/how-schools-can-prepare-artificial-intelligence-backed-cyberattacks

project tomorrow

iboss