K–12 Cybersecurity:

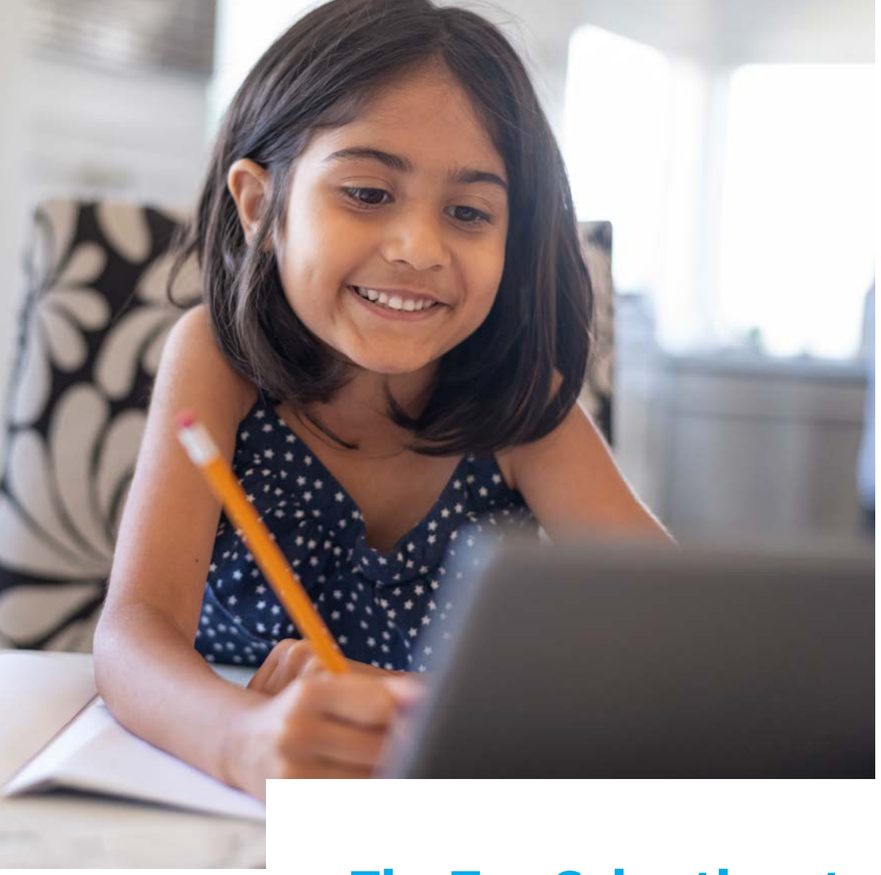
Creating a secure learning landscape

AT&T

In January 2022, a cyberattack forced Albuquerque Public Schools in New Mexico to cancel classes for some 75,000 students.[1] And, in a separate incident that same month, about 5,000 schools and colleges had their websites go dark when a ransomware attack hit a private company that provides web hosting services for education.[2]

These are among the latest security breaches to affect K–12 districts, which have become highly attractive targets for cybercriminals. The nonprofit K–12 Cybersecurity Resource Center counted 408 publicly disclosed cyberattacks against K–12 school systems in 2020, an 18% increase over the prior year.[3]

With cybersecurity only growing in importance, what are the key threats that K–12 districts face? What steps should school systems take to protect their networks and secure their data? Here are some important insights to help K–12 leaders create a more secure learning landscape.



The Top Cyberthreats for K–12

There are many threats to network and data security that K–12 leaders must be aware of. Here are some of the most common.

Distributed denial of service (DDoS): These brute-force attacks aim to overwhelm school district networks with more traffic than they can handle, thereby crippling the network.

When online learning greatly increased during the pandemic, education became one of the main targets for DDoS attacks worldwide—with the number of incidents rising 550% during the first quarter of 2020 alone.[4] The availability of DDoS-for-hire services gives hackers the ability to conduct disruptive DDoS attacks regardless of their experience level.

The disruption to network services caused by DDoS attacks can be "devastating for school districts," says Patrick Robinson, Associate Director of Cybersecurity for AT&T. "The Internet is a critical asset for K–12. To have the Internet completely disrupted is debilitating for the delivery of content, voice over IP and other web-based services."

Phishing: Phishing scams are becoming more sophisticated in nature, which is one reason why nearly half of K–12 IT leaders (45%) say phishing attacks are a significant security risk.[5] For example, it's becoming increasingly common for attackers to send an email message that looks like a note from a district administrator or another trusted person with whom the recipient feels comfortable sharing information.

Since 2016, the average amount of money stolen in certain types of phishing attacks specifically against K–12 administrative staff and vendors is about $2 million per incident.[6] But attackers aren't just looking for money. They're also phishing for students' personal information, including Social Security numbers.

"The identities of students, especially minors, are valuable on the Dark Web," Robinson observes. "Virtually no one tracks the credit status of minors, so they make an ideal target."

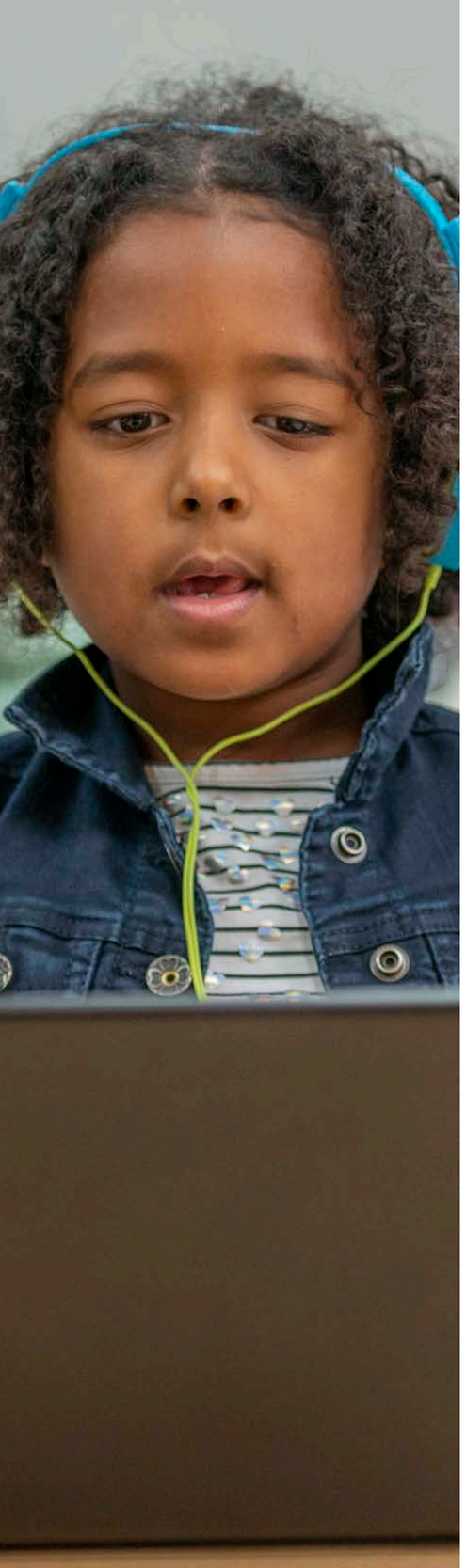
Ransomware: K–12 education has become the most frequently targeted sector for ransomware since the start of the 2020-2021 school year and now accounts for more than half of all ransomware attacks, according to the FBI and other security agencies.[7]

Not only are the numbers of ransomware attacks on K–12 schools on the rise, but so are the dollar amounts cybercriminals are demanding—in some cases far exceeding $1 million per incident. And in a new twist, the attackers are using the data they steal from networks as leverage for payment.[8]

"Charging the school district to release the data is an increasing occurrence," Robinson says. "Many districts pay the ransom just to have their data back."

"The Internet is a critical asset for K–12. To have the Internet completely disrupted is debilitating for the delivery of content, voice over IP and other web-based services."

Patrick Robinson—*Associate Director of Cybersecurity for AT&T*



Five Steps to Cybersecurity Success

Safeguarding student data and other critical information has become a top priority for K–12 administrators and leadership. Bolstering cybersecurity requires district leadership to commit significant time and resources to this critical issue. In doing so, districts should adopt a risk-based strategy for improvement, Robinson says.

In a risk-based approach, the central question is: What security risks does our school system face? Once districts have answered this question, they can make sound business decisions about where to spend money on IT personnel, technologies and controls that can help protect their critical infrastructure and data. Here are five key steps for success.

1 • Form a cross-functional task force.

The first thing school systems should do, Robinson says, is create a cross-functional cybersecurity committee or task force, with representation from both senior administration and IT.

Communication between the school board, superintendent's office and IT is essential. To execute the district's vision, IT operations must understand the expectations of the superintendent and school board with regard to the district's focus and its willingness to invest in cybersecurity measures. In turn, district leadership should understand what IT capabilities the district has in order to govern effectively. Involving both the executive and operational levels in collaborative planning creates a feedback loop that allows for successful security measures—in and out of the classroom.

"The biggest challenge to cybersecurity is a disconnect between leadership and IT operations," Robinson says. "When those who govern and those who operate aren't on the same page, it creates two separate mindsets. This fundamental breakdown in communication between the two groups is a serious issue."

2 •• Develop a cybersecurity charter.

Once school systems have created a cross-functional task force, the next step is to develop a vision and mission statement. "This is a statement that the district will hold itself accountable to," Robinson explains. "It becomes the working document that the cybersecurity committee can use to ensure they are aligned with senior leadership's expectations around cybersecurity."

3 ••• Assess risks.

A risk-based approach to cybersecurity involves assessing the risks that a district faces and then developing a plan to mitigate them. A risk assessment is best done by an independent third party, much like financial systems are audited by independent auditors. This third party should have expertise in cybersecurity audits, and they should follow a standard security audit process. The result of the assessment is a formal, unbiased identification of a district's cybersecurity vulnerabilities.

4 •••• Create a plan.

Once the district's security gaps have been identified, the cybersecurity task force can put together an action plan for addressing them. The action plan should establish clear goals and a schedule for prioritizing these goals. The plan should specify who's responsible for which steps and set target dates for their completion.

5 ••••• Measure progress.

The action plan creates a roadmap for improvement. To ensure success, districts need to monitor their progress toward the plan's objectives. As school systems do in other aspects of their operations, they should develop key performance indicators (KPIs) around cybersecurity as well.

In addition, districts should establish a regular cadence for identifying cybersecurity risks moving forward. For example, how often will the district conduct a formal risk assessment? How often will IT personnel scan the network for vulnerabilities? How often will the district conduct penetration testing to make sure the network is secure?

"Generally speaking, a risk assessment is a large exercise," Robinson says. "It rarely takes place every year. A common best practice is to conduct a full risk assessment every three years or so. Network scanning could occur as frequently as weekly, depending on the size of the district and the resources it has available. More commonly, you'll find that districts might do this twice a year, or perhaps once a month if they're more aggressive. Critical assets might be subjected to some kind of penetration testing once a year to make sure they meet basic standards of security."

Moving Toward ‘Zero Trust’ Security

Adopting a risk-based strategy is a more proactive approach to cybersecurity than simply responding to threats or attacks as they occur, Robinson says. For school systems that are further along in the cybersecurity continuum, the next evolution is to embrace a “zero trust” mindset.

“Zero trust is not a technology. It’s more of a philosophical approach to cybersecurity in which we assume that no user, device or network element is inherently trustworthy,” he explains. “So, we rebuild existing network systems to require proof at every step of the way that a user or device can be trusted. This is an ideal state, but it’s also a long-term and somewhat expensive process. For larger school systems and those who are very good at risk-based management today, zero trust should be the next major objective.”

Zero trust security involves authenticating users or devices whenever they try to access the network, verifying the identity of those users or devices and then tracking their use of the network at every step.

“In a typical network environment, a user logs onto the network, and we just assume that the person we expect to see is actually behind those login credentials,” Robinson says. “In a world of zero trust, we don’t assume any of that. We verify through additional layers of security that it is, in fact, the employee or student we had expected to see. Only when we’re satisfied do we allow them to perform their work.”

Zero trust requires the use of identity and access management technologies. For school systems that are already handling risk-based management well, zero trust should be their next cybersecurity objective.

Stimulus Funding and K–12 Cybersecurity

Since March 2020, federal lawmakers have passed three emergency aid packages that collectively provide more than $189 billion in funding for K–12 education through the Elementary and Secondary School Emergency Relief (ESSER) Fund, in the Education Stabilization Fund (ESF).[9]

With cyberattacks against K–12 districts on the rise even before the pandemic emerged and the shift to remote learning during COVID-19, the question was posed in the ESSER FAQs about whether ESSER funds could be used to improve cybersecurity. According to federal guidance,[10] if a school or district “is improving cybersecurity to better meet [the] needs of students related to preventing, preparing for or responding to COVID-19,” then it may use ESSER funds for this purpose.

The guidance continued to state, “For example, if an LEA needs to increase its use of technology, such as for potential temporary shifts to hybrid learning if COVID-19 cases arise, expanded cybersecurity needs to facilitate that activity may also be addressed using ESSER…”

As K–12 leaders consider how to best safeguard and protect network infrastructure and student data—in and out of the classroom—the $189 billion in federal emergency relief aid offers a potential opportunity for schools to assess and address their cybersecurity needs now.

The Time Is Now

With cybercriminals increasingly targeting K–12 school systems, cybersecurity has become a vital issue. As school leaders and district administrators balance their ever increasing list of priorities—detecting, responding to, and preventing cyber threats requires attention and resources—and are too important to be overlooked.

Adopting a risk-based approach is the first step in improving cybersecurity. To do this effectively, leadership and IT teams should work together to create and execute a plan that is based on an objective, third-party risk assessment. For districts that are more advanced in their approach, "zero trust" security is the next logical step in keeping networks and data secure.

While K–12 budgets are often stretched thin, the pandemic has created a unique opportunity for school systems to assess, fortify and strengthen their cybersecurity defenses. As Districts embrace a return to better, not just normal, enabling a more secure learning environment for students and staff is key.

---

1 "A cyberattack in Albuquerque forces schools to cancel classes," NPR, Jan. 14, 2022. https://www.npr.org/2022/01/14/1072970219/cyber-attack-in-albuquerque-latest-to-target-public-schools

2 "Thousands of School Websites Went Down in a Cyberattack. It'll Happen Again, Experts Say," Education Week, Jan. 10, 2022. https://www.edweek.org/technology/thousands-of-school-websites-went-down-in-a-cyberattack-itll-happen-again-experts-say/2022/01

3 "The State of K–12 Cybersecurity: 2020 Year in Review," K–12 Cybersecurity Resource Center, March 2021. https://k12cybersecure.com/wp-content/uploads/2021/03/StateofK12Cybersecurity-2020.pdf

4 "DDoS Attacks on the Educational Sector are Threatening Online Learning," Cybersecurity Magazine, Nov. 8, 2021. https://cybersecurity-magazine.com/ddos-attacks-on-the-educational-sector-are-threatening-online-learning/

5 "The State of EdTech Leadership 2021 Survey Report," Consortium for School Networking (CoSN). https://www.cosn.org/tools-and-resources/resource/edtech-leadership-survey-report-2021/

6 "The State of K–12 Cybersecurity: 2020 Year in Review."

7 "K–12 Has Become the Most Targeted Segment for Ransomware," T.H.E. Journal, Dec. 11, 2020. https://thejournal.com/articles/2020/12/11/k12-has-become-the-most-targeted-segment-for-ransomware.aspx

8 "The State of K–12 Cybersecurity: 2020 Year in Review."

9 U.S. Department of Education, "Education Stabilization Fund,". https://covid-relief-data.ed.gov/

10 U.S. Department of Education, "Frequently Asked Questions: Elementary and Secondary School Emergency Relief Programs," May 2021. https://oese.ed.gov/files/2021/05/ESSER.GEER_.FAQs_5.26.21_745AM_FINALb0cd6833f6f46e03ba2d97d30aff953260028045f9ef-3b18ea602db4b32b1d99.pdf

cybersecurity.att.com