GUIDE

How to stay a step ahead of cybersecurity threats in K-12 education

The digitization of K-12 education — widespread internet access, increased use of mobile devices, online learning and smart classroom tools — helps schools reach their education goals. Use of Internet of Things (IoT) devices like sensors for energy conservation and security can contain costs and streamline school management. While these important changes enhance teaching and improve operations, they create a huge surface for cyberattacks.

According to Consortium for School Networking (CoSN), cybersecurity and student data privacy are ranked as the top two priorities for school district IT leaders.[1] Yet, district IT leaders generally underestimate the threats to K-12 networks. The vast majority (84 percent) don't rate any cybersecurity threat as a high risk — and just 41 percent of districts have a cybersecurity plan.[2]

Lean budgets, aging network infrastructure and the growing sophistication of cybercriminals have driven up the number of attacks year over year. Data security incidents in K-12 schools increased by 18 percent in 2020.[3]

The ongoing digital collection and aggregation of student and staff data is extremely attractive to cybercriminals. Consider these statistics:

- **1,164** cyberattacks have occurred in K-12 districts in the last five years.[4]
- **24.5 million** student records have been compromised in cyberattacks since 2005.[5]
- **> 60 percent** of worldwide cyberattacks target educational institutions.[6]

To change their risk profile, K-12 schools and districts need to adopt new network security practices.

24.5 million

student records have been compromised in cyberattacks since 2005.[7]

IoT devices are the new vector of choice for cybercriminals, meaning if your school has sensors, smart locks, digital learning tools or other infrastructure connected to your network, you may be at higher risk.

Tracking evolving threats

Although the profile of threats is concerning, you can protect your district from attacks that come from a wide range of attack vectors. Understanding current and emerging types of threats can help you put the right protection in place.

Phishing: Around half (45 percent) of K-12 tech leaders say phishing scams are a significant risk.[8] This is likely because phishing scams have become more sophisticated. Recipients used to click on an attachment to be phished, but these days, the payload can be an innocuous-looking link embedded in the email itself. And, it's becoming increasingly common for hackers to set up the email to look like a note from a district administrator or another trusted person with whom the recipient is comfortable sharing the requested information. Since 2016, the average amount of money stolen in phishing attacks against K-12 administrative staff and vendors is $2 million per incident.[9]

Malware and viruses: Hundreds of thousands of malware deviations appear each year, including keyloggers that record all keystrokes typed and password-stealers that extract all passwords saved and send them to hackers. Polymorphic and metamorphic malware are designed from the get-go to change nearly all the time. One type of malware lets the hacker view, delete and download files; another turns on a webcam to spy on the recipient.

Volumetric distributed denial of service (DDoS): These brute-force attacks are throwing more traffic via more vectors at district networks than ever before. They're combining volumetric, session-exhaustion and application-layer attack vectors. In session-exhaustion attacks, the firewall is essentially turned inside-out, becoming a tool for the hackers instead of a network defense. Application-level attacks target the code that runs the website or application. In December 2020, the FBI and other security agencies issued a warning to K-12 districts that stated: "Cyber actors are causing disruptions to K-12 educational institutions … with distributed denial-of-service (DDoS) attacks, which temporarily limit or prevent users from conducting daily operations. The availability of DDoS-for-hire services provides opportunities for any motivated malicious cyber actor to conduct disruptive attacks regardless of [their] experience level."[10]

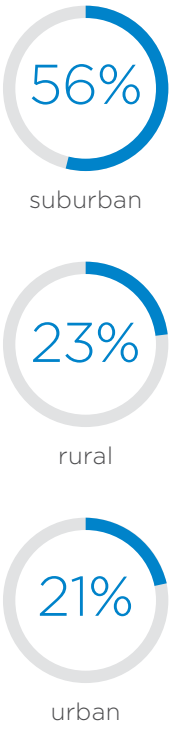
Ransomware: Not only are the numbers of ransomware demands increasing, so are the dollar amounts required to set your network free — in some cases far exceeding $1 million per incident.[11] What's more, a newer variety of ransomware threatens to release your information publicly if you don't pay. IoT devices are the new vector of choice for cybercriminals, meaning if your school has sensors, smart locks, digital learning tools or other infrastructure connected to your network, you may be at higher risk.

Data breach: It isn't new that bad actors are stealing personally identifiable information (PII) — names, addresses, phone numbers, Social Security numbers (SSNs) and other data — then selling it on the dark web. Criminals' innovation, though, is to corrupt rather than steal from school databases. In this scenario, hackers might delete database tables, change records or erase entire databases.

Real-world cyberattacks

Details of K–12 cybercrimes help to paint a clear picture of the evolving threat. Read these examples and see how schools might have been better protected against an attack.

Cyberattacks by community type, 2016-2020[12]



Ransomware attack takes down school website

Type of breach: A ransomware attack.

What was lost: Email, lunch payment services and the school's website were incapacitated; the ransom was paid in bitcoin after six days, but the hackers didn't release the files for weeks afterward. All the district's computers in the town were also unusable during that time.

What might have mitigated or thwarted the attack: Multifactor authentication and segmented security zones within the network could have hindered bad actors from moving laterally if they gained access to one device. Use of anti-virus software and a next-generation firewall, as well as content scanning and filtering on mail servers, could have protected critical data and prevented intrusion.

Third-party app allows entry into school's computer system

Type of breach: Phishing/data compromise.

What was lost: A hacker sent emails to employees of a third-party medical-benefits vendor, and one staffer responded. As a result, personal information about employees of an entire school district — including full SSNs for three school employees and the last four digits for around 600 others, along with addresses and birthdates for all — was hacked. It's possible the hackers figured out full SSNs for all school employees with just the data they had.

How the breach could have been prevented: Use of anti-malware protection and a next-generation firewall may have prevented the attack. Encrypted data, both in transit and at rest, would have rendered all the district's PII as unreadable. A knowledgeable internet provider would have the technology and expert staff available to ensure this.

DDoS attacks shut down 50 districts

Type of breach: Volumetric DDoS attacks.

What was lost: The technology services center for 50 school districts was shut down nine times during a six-month period by DDoS attacks. Students and teachers lost access to educational materials, officials had to devote significant resources to addressing the attacks and roughly 25,000 students were unable to take the state English assessment tests.

How the breach could have been prevented: DDoS security protection services could have blocked the offending IP address and prevented secondary attacks. With the address blocked, clean traffic would be allowed to pass, which would have enabled city sites to continue operations.

Finding the right protection for your school or district

Continually keeping ahead of cybersecurity threats to your network requires comprehensive and coordinated coverage. That includes firewalls, unified threat management (UTM), DDoS protection and the support of a network services provider to deliver managed service solutions.

When it's time to evaluate a provider and its services, ask the following questions to help you find the best protection possible:

- How can you safeguard us against malware, phishing and other common cyberattacks?
- How do you identify and mitigate network threats? Can you scan our network for attacks and drain suspicious traffic?
- What protection do you provide against volumetric DDoS attacks?
- Do you have a means of letting us continue to work productively after a DDoS attack on the parts of the network that were not affected?
- Do you provide UTM? What protection does that provide?
- Can your firewall protect traffic between our various sites as well?
- Is a next-generation firewall part of what you offer? What protection does it provide?
- Do you have an integrated solution that includes firewall, UTM and internet service to simplify protection?
- Threats are evolving, and our network is always changing and growing. Can you support us and our investment as the environment and our needs change?
- How can you offload day-to-day administration work from our IT team during and after implementation?
- What types of teams and experts will we have access to for service? Are they available 24/7/365?

Comprehensive coverage and support

Widespread, coordinated network protection can keep you one step ahead of evolving and growing K-12 network threats. You can balance the needs for complexity in coverage and simplicity in operation by choosing security as a managed service. With the right partner, you're supported from design through implementation and provided with ongoing support. See how Spectrum Enterprise is uniquely qualified to protect your district's network.

Learn more

1. "The State of EdTech Leadership 2021 Survey Report," Consortium for School Networking (CoSN), 2021.
2. Ibid.
3. "The State of K-12 Cybersecurity: 2020 Year in Review," K-12 Cybersecurity Resource Center, March 2021.
4. Ibid.
5. "What happens when private student information leaks," The Hechinger Report, Nov. 9, 2020.
6. "Global threat activity," Microsoft, Accessed Aug. 10, 2021.
7. "What happens when private student information leaks," The Hechinger Report, Nov. 9, 2020.
8. "The State of EdTech Leadership 2021 Survey Report," Consortium for School Networking (CoSN), 2021.
9. "The State of K-12 Cybersecurity: 2020 Year in Review," K-12 Cybersecurity Resource Center, March 2021.
10. "Joint Cybersecurity Advisory: Cyber Actors Target K-12 Distance Learning Education to Cause Disruptions and Steal Data," Federal Bureau of Investigation (FBI), Cybersecurity and Infrastructure Security Agency (CISA) and Multi-State Information Sharing and Analysis Center (MS-ISAC), December 2020.
11. "The State of K-12 Cybersecurity: 2020 Year in Review," K-12 Cybersecurity Resource Center, March 2021.
12. Ibid.

About Spectrum Enterprise

Spectrum Enterprise, a part of Charter Communications, Inc., is a national provider of scalable, fiber technology solutions serving many of America's largest businesses and communications service providers. The broad Spectrum Enterprise portfolio includes networking and managed services solutions: Internet access, Ethernet access and networks, Voice and TV solutions. The Spectrum Enterprise team of experts works closely with clients to achieve greater business success by providing solutions designed to meet their evolving needs. For more information, visit enterprise.spectrum.com.

Spectrum ENTERPRISE