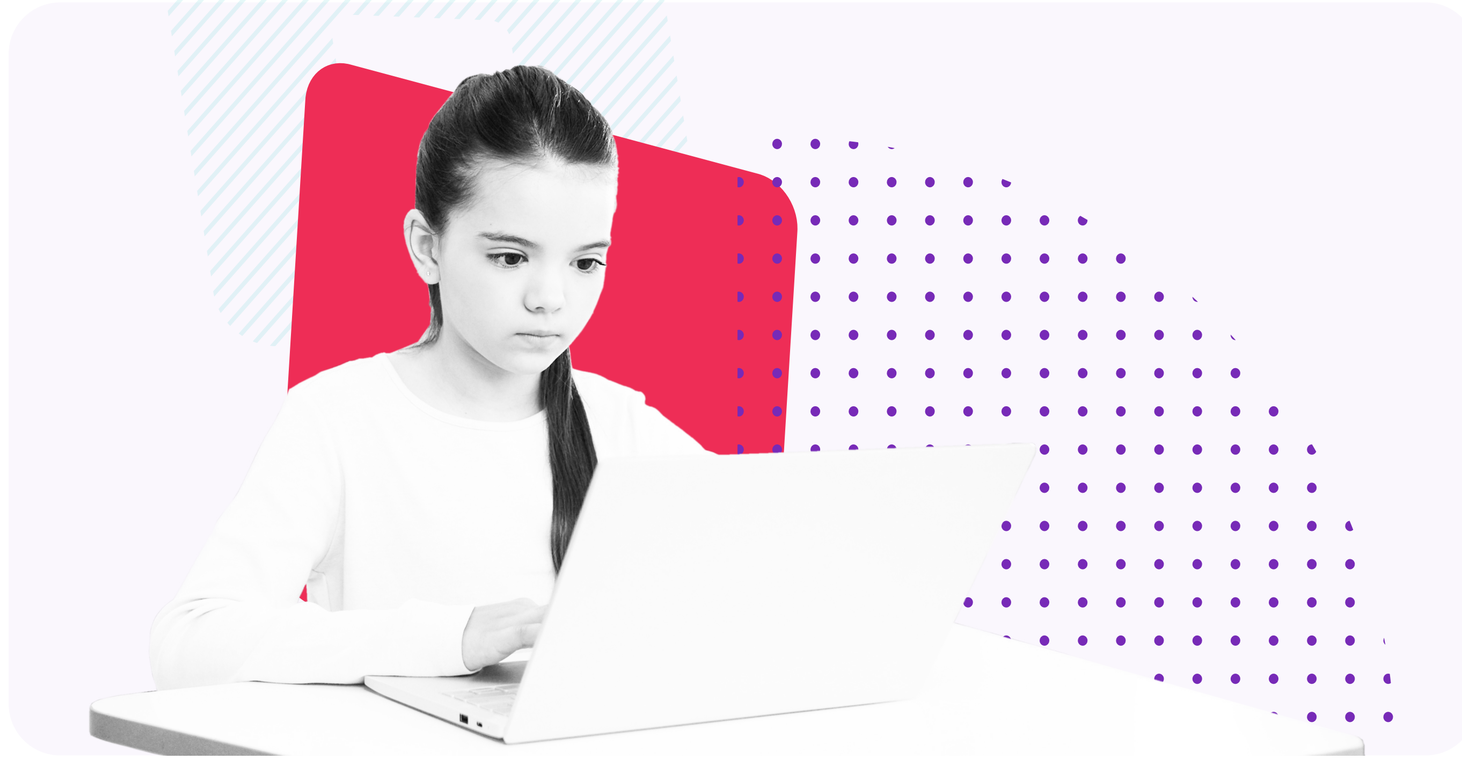


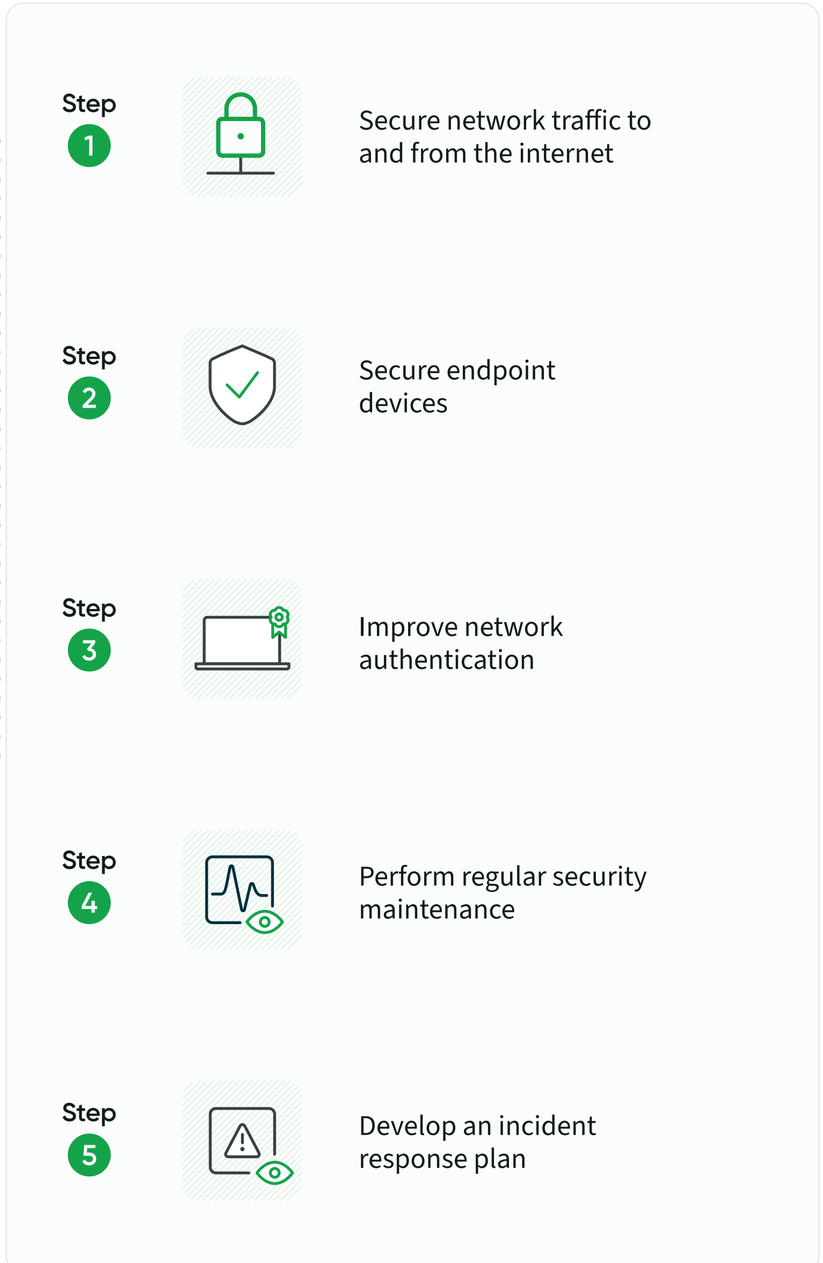
WHITE PAPER

5 Cybersecurity Practices Every K-12 District Should Follow

Cybersecurity Basics for Every K-12 District

Cyberattacks against K-12 school systems are on the rise. With valuable information such as students' names, birth dates, and Social Security numbers on file, K-12 school systems make highly attractive targets for cybercriminals. Yet, many school systems still lack even basic cybersecurity policies and controls that could protect them from an attack.

A network security breach can be quite costly for schools. Beyond the financial expense involved in restoring networks and data systems to their original state, student data privacy is also at risk. School districts are responsible for safeguarding sensitive information, and the theft of students' personal information can cause irreparable damage to a district's reputation. A ransomware attack or other security breach can also cripple operations, bringing teaching, learning, and school administration to a halt.



School systems must adopt fundamental strategies for shielding their networks from attack, such as implementing software to protect against malware and viruses and ensuring these key applications are working correctly.

The Need for K-12 Cybersecurity

As the number of students using digital devices for learning has grown dramatically over the last few years, the opportunities for cybercriminals to wreak havoc on K-12 networks have multiplied as well.

A 2022 Consortium for School Networking (CoSN) survey revealed cybersecurity is the number one technology pain point for school systems. Additionally, 83 percent of respondents work in school systems that will be expanding cybersecurity initiatives.

The K-12 Cybersecurity Resource Center reports that there has been a steady increase in the frequency and severity of cyberattacks targeting K-12 schools systems, and 2020 was the worst year yet with at least 408 publicly disclosed incidents—up 18% from 2019.[1] Common threats that continue to plague schools include accidental or intentional data breaches, ransomware attacks, and Distributed Denial of Service (DDoS) attacks.

Ransomware attacks on K-12 networks are becoming more sophisticated. “Criminal actors aren’t just locking systems, they’re stealing personally identifiable information,” says Doug Levin, who heads the K-12 Cybersecurity Resource Center. “This increases their leverage over the district to meet their demands, and—whether or not the ransom is paid—they may still try to monetize the data.”

In addition, ransomware demands have risen dramatically. In Broward County, Florida, hackers demanded $40 million.[2]

While many school systems rely on insurance providers as a backstop for these kinds of incidents, insurance premiums for ransomware policies have skyrocketed in recent years, Levin says. He adds: “Insurers have started requiring school districts to put into place a large array of cybersecurity controls in order to even qualify for insurance.”

Cybersecurity Basics for Every K-12 District

Even though cybersecurity is a top-of-mind issue, many school systems aren't being proactive enough in guarding against cyberthreats. Several districts are either understaffed or lack the necessary knowledge or skills to create an effective cyberdefense strategy. In some cases, district leaders might feel they have too many competing priorities to pay enough attention to cybersecurity.

Because there are no formal cybersecurity standards for schools, K-12 leaders can feel overwhelmed by all the advice that exists. They might not know where to begin.

But cybersecurity doesn't have to be complicated. There are some basic steps that every school system should take to keep its networks and data secure. Here are five fundamental steps that districts should implement right away if they haven't already.

1. Secure network traffic to and from the internet

Making sure network traffic to and from the internet is secure involves using firewalls and internet security software to filter out malware; looking for phishing emails and trying to quarantine them; restricting the downloading of macros in documents, which are a common vehicle for ransomware; and limiting the use of internet-facing services that are constantly connected.

"The FBI issued an alert earlier this year, warning of attacks that exploit the Remote Desktop Protocol service that allows a tech support person to log into someone else's computer to work on it," Levin notes. "Basically, if a school district has a server or a system that doesn't need to be exposed to the internet, those systems should be shut off or protected in some way."

2. Secure endpoint devices

Laptops, tablets, and other devices also must be secured. School districts should protect student, staff, and teacher devices by restricting administrative access on those machines, so users can't just install whatever software they'd like.

The devices themselves also need endpoint protection, such as anti-virus and anti-malware software. K-12 leaders should make sure these endpoint security controls are working at all times by investing in platforms that make them resilient—that is, self-aware and capable of maintaining their effectiveness automatically.

Districts should have continuous access to geolocation data both on and off their network. If a device goes missing, they should be able to lock it, freeze it, and remotely wipe any sensitive information to ensure they remain compliant with the Family Educational Rights and Privacy Act (FERPA) and other privacy regulations.

"Districts should have continuous access to geolocation data both on and off their network. If a device goes missing, they should be able to lock it, freeze it, and remotely wipe any sensitive information."

DOUG LEVIN,
K-12 CYBERSECURITY RESOURCE CENTER,

3. Improve network authentication

The authentication practices that schools use for granting network access need better security. K-12 leaders should train students and employees in best practices for establishing and using strong passwords, such as creating passwords that are hard to guess but easy to remember, never sharing passwords with others, and using different passwords for different accounts. School districts should consider other measures to improve authentication as well, such as requiring multifactor authentication and adopting single sign-on technology.

“Anything that schools can do to prevent password compromise, sharing, and reuse will go a long way toward keeping data safe,” Levin says.

4. Perform regular security maintenance

Cybersecurity should be an ongoing area of focus. School systems should regularly back up critical data, install security updates and patches in a timely manner, test their security defenses to make sure these are working properly, audit their systems and data to see where vulnerabilities might exist, and review the sensitive data they’re storing to see what can be archived or deleted.

“Some of the largest security breaches involving school districts include data not just about current students and staff, but those who might have interacted with the district five or 10 years ago,” Levin says. “If older information can be archived or even deleted, that reduces the potential surface area for an attack.” Encrypting all sensitive information and deleting information that is no longer necessary to maintain are best practices for ensuring FERPA compliance.

5. Develop an incident response plan

Another fundamental step that every district should take is to create or update an incident response plan so that if an attack does occur, employees know how to react.

“There’s no such thing as 100-percent security,” Levin says. “At the end of the day, if an attacker is patient, tech-savvy, and highly motivated, it’s going to be very difficult for school districts to keep their data systems fully secure. Even the largest and most well-resourced companies and government agencies have trouble doing that. This is why it’s critical for school districts to create a plan, take steps to defend themselves, and practice their plan so they’re well prepared if their defenses are breached.”

A thorough cybersecurity plan should ensure that everyone knows his or her role in the event of an attack. District leaders should know who they’re going to call for help, such as their IT vendors and/or a third-party specialist who can help them respond. IT leaders should conduct routine scans to identify where all sensitive information is stored.

They should regularly back up all data and delete any information stored on unprotected devices. In addition, leaders should know how they’re going to communicate a data breach to their community.

“That’s definitely not something you want to be figuring out in the heat of the moment,” Levin says.

There is no magic bullet for protecting K-12 networks and data from attacks. However, by taking these five fundamental steps, school districts can improve their cybersecurity dramatically.

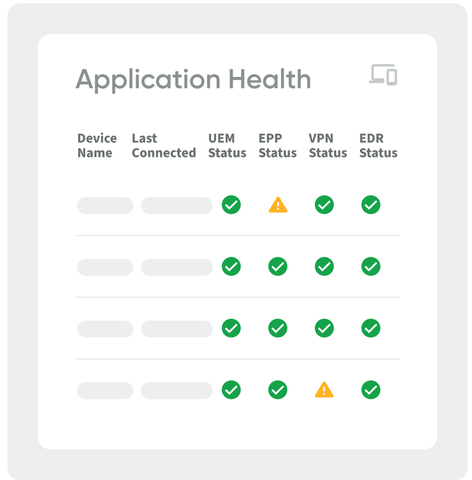
The time to act is now

Cybersecurity threats aren’t going away; in fact, they are only going to get worse. School systems need to take these threats seriously—and implementing these five steps is a good start.

“School districts should aim to become more secure tomorrow than they are today,” Levin concludes. “As schools come to rely more on technology, they will continue to be victimized unless they pay more attention to this critical issue.”

“Some of the largest security breaches involving school districts include data not just about current students and staff, but those who might have interacted with the district five or 10 years ago.”

DOUG LEVIN,
K-12 CYBERSECURITY RESOURCE CENTER,



How Absolute can help

The Absolute Platform for Endpoint Resilience® helps schools and districts ensure that their devices and security controls maintain a secure operational state automatically, without the need for user intervention. Here are three ways that Absolute can help schools protect their networks and data more effectively.

Endpoint security and device recovery

Lost or stolen devices can be exploited by bad actors to gain access to networks or data. Absolute's software includes tools that enable schools to wipe or freeze devices that go missing, as well as tools that aid in tracking and recovering lost or stolen devices.

Application functionality

Encryption, anti-virus, and anti-malware software can only provide protection if they're working effectively. If these programs are disabled or not functioning, then school networks and data are vulnerable to an attack. Often, when hackers gain access to a computer system, they'll disable the software protecting the rest of the network. According to Absolute's "Endpoint Trends in K12 Education 2021-22" report, only 53% of the anti-virus applications studied were operating effectively.[3]

If Absolute's software detects that an endpoint device's security solutions have been uninstalled or aren't working correctly, it will reinstall these solutions automatically. By ensuring the integrity of security applications, Absolute's software removes the burden from IT staff to check and maintain these systems manually.

Scanning for sensitive information

Often, educators aren't even aware they are storing sensitive information on endpoint devices and other vulnerable locations. Nearly one-third of the education devices studied for Absolute's "Endpoint Trends in K12 Education 2021-22" report contained sensitive data such as Social Security numbers and student health information.[4]

Absolute's software helps schools determine whether they are at risk from unencrypted data. The software scans devices to look for personal health information, Social Security numbers, financial information, and other sensitive data stored on these machines. K-12 leaders can schedule and run regular reports to see which devices contain unprotected data, so they can take steps to secure this information.

1 K-12 Cybersecurity Resource Center (2021). "The State of K-12 Cybersecurity: 2020 Year in Review."

2 Goodhue, David (2021). "Hackers breach Broward schools' computer system. They're demanding millions in ransom." The Miami Herald.

3 Absolute Software (2021). "Endpoint Trends in K12 Education 2021-22."

4 Ibid.

eSCHOOL NEWS.com

This white paper was produced by eSchool News, the online platform that delivers daily technology news and information to K-12 education administrators, educators, and technology professionals, and dedicated to the advancement and wise use of technology to improve teaching and learning for all. eSchool News offers ed-tech decision makers a wide range of informative content — including newsletters, webinars, case studies, white papers, websites, and more — that provide in-depth coverage of the latest innovations, trends, and real-world solutions impacting the education community. Explore more at www.eSchoolNews.com.

ABSOLUTE®

Absolute Software makes security **work**. We empower mission-critical performance with advanced cyber resilience. Embedded in more than 600 million devices, our cyber resilience platform delivers endpoint-to-network access security coverage, ensures automated security compliance, and enables operational continuity. Nearly 21,000 global customers trust Absolute to protect enterprise assets, fortify security and business applications, and provide a frictionless, always-on user experience.

Request a Demo