Securing the Future:

How Schools and Districts Stay One Step Ahead of Cyber Threats

ActZero
a WatchGuard brand

actzero.ai

OVERVIEW

Educational technology leaders, the unsung heroes who ensure the seamless functioning of school technology, face a paramount challenge: the escalating threat of cyberattacks. CoSN's 2023 K-12 EdTech Leadership Survey reveals the threat of a cyberattack has remained the top priority over the past five years.

Every school district grapples with vulnerabilities, especially in safeguarding student data targeted by cybercriminals. However, small and rural schools are at a greater disadvantage in proactively protecting against cyberattacks, due to a lack of resources and expertise. Nearly half of U.S. school districts have an enrollment that does not exceed 1,000 students; more than 70 percent of districts enroll fewer than 2,500 students.

According to the same CoSN survey, only one-third of districts allocate a full-time employee to network security, leaving two-thirds feeling inadequately equipped to tackle cyber threats. In response, practical measures such as heightened awareness, staff training, and strategic investments are advocated to fortify districts, particularly those with constrained resources.

The surge in ransomware further compounds risks, making K-12 the top-targeted sector. In 2023, there were 102 education-related ransomware attacks through mid-September alone, emphasizing the urgency for proactive measures and reliable security partnerships. Ransomware attacks, constituting over 30% of breaches in education, result in significant educational and monetary losses.

According to a 2022 U.S. Government Accountability Office report, the aftermath of a cyberattack can lead to as many as three weeks of learning loss, with recovery taking two to nine months. Financially, school districts have suffered losses ranging from $50,000 to $1 million per cyberattack. The imperative for robust cybersecurity measures and collaborative efforts to protect student data is underscored by the substantial impact of these attacks on both education and finances.

Reacting isn't enough, as a single ransomware attack can close school and leave your students' data compromised. Sophisticated attacks launched by adversaries around the world emphasize the need for proactive measures and trusted security partnerships.

WHAT IS CONSIDERED A TARGET?

From 2016 to 2022, the K12 Security Information Exchange (K12 SIX) logged a total of 1,331 publicly disclosed cyber incidents affecting U.S. school districts. This equates to a rate of more than one K-12 cyber incident per school day experienced by the nation's public schools—and districts of all sizes and geographic areas are at risk.

"School districts from all 50 states have suffered significant cyber incidents, from very small, rural districts to the largest urban school districts in the nation," K12 SIX noted in its 2022 "State of K-12 Cybersecurity: Year in Review" report.

Cloud Security and Data Loss

As school systems modernize their IT infrastructure by moving away from data centers and workstations and toward solutions such as cloud service providers, SaaS delivery models, and thin clients, attackers are pivoting from disruption to extortion and data extraction, targeting cloud-based systems to steal data and extort your school or district by placing this information on the Dark Web. Combating this requires the use of different monitoring tools like Cloud Security Posture Management (CPSM), Cloud Workload Protection Platforms (CWPP), and agents on any managed devices used by students and employees that can detect such attacks, many of which bypass multi-factor authentication (MFA)—like a pass-the-cookie attack.

Locally Hosted Software

Although IT modernization is under way, many districts still rely on locally hosted software to store, process, and transmit the student and staff data required for daily operations. These systems inherently provide more risks in data protection and recovery, because they rely on under-resourced districts to monitor, manage, and secure their servers and other IT infrastructure;

install regular software updates and security patches; and restore and rebuild systems in the event of an attack. The more mission-critical the application, the more attractive it is for attackers to disrupt.

Smaller Organizations Especially at Risk

Looking at wider trends, the demographics for targets tend to favor smaller organizations with fewer tools, processes, or IT personnel to monitor or recover from an attack. In fact, 82% of ransomware attacks focus on organizations with fewer than 1,000 employees. K-12 leaders within smaller school systems might think no one is coming for their data, but in reality they face just as much risk as larger districts.

Most Attacks Happen Off-Hours

Hackers work outside of normal business hours. In fact, 76% of ransomware attacks occur off-hours or on weekends. This provides a window of opportunity to attack when team members are away, and it ensures that systems offline or disconnected from the network can be infected quickly upon return. With attackers only requiring 84 minutes, on average, to spread the initial infection to other systems across the data center, the ideal time to attack is the late evening prior to a holiday weekend return.

HOW ARE SCHOOLS BEING ATTACKED?

The 1,331 publicly disclosed cyberattacks that K12 SIX has cataloged against school districts from 2016 to 2022 include a wide array of incident types, including:

- **Ransomware attacks**, in which cybercriminals attempt to extort money from their victims by holding data hostage.
- **Phishing attacks**, which trick users into divulging sensitive information. The most common types of phishing attacks against K-12 districts are business email compromise (BEC) scams, involving the use of email to scam school business officials or other staff members out of sensitive information and/or millions of dollars of money—such as by issuing fake invoices to districts, redirecting authorized electronic payments to bank accounts controlled by criminals, or stealing the W-2 tax information of district employees.
- **Distributed Denial of Service** (DDoS) attacks, which aim to make school IT resources unavailable to students and staff by overwhelming these resources with network traffic to disrupt their normal functioning.
- **Website and social media defacement**, which involves making unauthorized changes—like posting inappropriate language or images—to a school or district website or official social media account.

The Escalating Challenge of Ransomware Attacks for Schools

Many district leaders might assume they're most vulnerable from disgruntled employees or students hacking into their systems. The truth is, the biggest threats come from professional cybercriminals who are increasingly targeting K-12 districts. Ransomware attacks on K-12 schools have been on the rise in recent years. From 2018 to mid-September 2023, at least 561 educational institutions were hit by a ransomware attack, Comparitech reports—costing an estimated $53 billion in downtime alone.

While ransomware attacks across other sectors dipped in 2022, education saw a rise in these types of attacks. During the first half of 2023 alone, Comparitech recorded at least 85 publicly disclosed ransomware attacks on schools and colleges worldwide—up from 45 in the same period of 2022. These attacks can have a devastating impact on schools—disrupting operations, compromising sensitive data, and costing millions of dollars in remediation costs.

What's more, ransomware attacks on K-12 schools are becoming more sophisticated in nature as attackers are increasingly using double extortion tactics. This involves both encrypting and stealing data, while threatening to release it if the ransom isn't paid.

Schools need to take concrete steps to protect themselves from these attacks. Solutions should include not only preventive measures that keep an attack from occurring, but also technologies that can detect an attack in progress and quarantine affected IT systems to stop the spread and minimize the damage.

WHERE ARE THE GAPS IN YOUR DISTRICT?

While every district's needs and circumstances are different, here are some of the most common challenges affecting K-12 cybersecurity.

Cost-Based Compromises

Budgets are always a challenge in K-12 education. According to CoSN's survey, only a third (32%) of IT leaders feel their school system has sufficient resources to stave off cybersecurity risks. With cybersecurity licensing, staffing, implementation, and monitoring costs rising, many organizations face difficult trade-offs in protection. Systems such as anti-malware products are amortized and might not be capable of detecting current-state attacks. Other key systems, such as firewalls or cloud products, are not logging activity centrally or monitored by external teams.

Slow Patching, Poor Configuration

Vendor-identified vulnerabilities are one of the most common ways for an attacker to infiltrate IT systems. Many organizations don't deploy vendor-released security patches automatically, nor do they implement best-practice configurations to systems. Remaining consistent and prioritizing this work is an essential yet often overlooked aspect of day-to-day IT work.

Identity Protections

Identity and access management (IAM) is the barbed-wired defense that protects a school system's data and assets by continually requesting credentials to verify a user's identity before granting network privileges. Basic username and password authentication systems are inadequate for the brute-force attacks employed by today's malicious actors. Furthermore, username and password combinations are easily procured by malicious actors on the Dark Web—giving them easy access to school and district IT systems.

'Tool Sprawl' and IT Complexity

School and district IT directors typically add new tools to their technology stack over time. Although each investment addresses a new operational challenge, this piecemeal approach often snowballs into an avalanche of alerts and a host of various systems to monitor and manage, with new tools that require patching and configuring to protect.

User Education

A study of recent cybersecurity incidents across all sectors found that the "human element" continues to drive many data breaches. Yet, CoSN's survey revealed that 13% of school districts don't provide cybersecurity training for their teachers, 12% don't provide this for administrators, and 33% don't provide it for students.

Ability to Monitor and Respond During Off-Hours

Since bad actors attack when most staff aren't working, K-12 IT leaders need to be confident their security teams can detect and respond to attacks at any time of day or night, specifically during off-hours or weekends. According to Gartner, 60% of organizations will use some kind of remote threat disruption and containment capabilities to help protect against threats by 2025. However, this number is only around 30% today.

Sampling of Cyber Incidents for Smaller & Rural Schools

District	Student Population	Details
Allen Park Public Schools, Michigan	3,701	In October 2023, the school district experienced a cyberattack, leading to the temporary shutdown of network segments and class cancellations. A third-party investigation is underway to assess the incident and address the issues, with full functionality expected to be restored in a few days. The extent of potential personal information breaches is currently unknown.
Hopewell Area School District, Pennsylvania	2,055	In October 2023, the Hopewell Area School District experienced a sophisticated ransomware attack, prompting the shutdown of certain network functions.
Crown Point Community School Corporation, Indiana	8,819	Crown Point Community School Corp. faced a cybersecurity breach in November 2023, costing approximately $1 million. Originating from a phishing email, the ransomware attack led to encrypted files and a one-day class cancellation. After negotiating a ransom payment, the district investigated potential data access, finding no compromise of financial information.
Newton Public Schools USD 373, Kansas	3,274	Newton Public Schools USD 373 canceled classes for two days in March 2023 due to a "network security incident."
Lebanon School District, Pennsylvania	1,635	The student-information and payroll systems of the Lebanon School District were taken offline following a ransomware attack. Students weren't able to access their final grades until July.
Chambersburg Area School District, Pennsylvania	9,118	The district was hit with a ransomware attack in August 2023. Later in October, they discovered during the investigation that certain personal data was compromised before containment.
Franklin County Public Schools, Virginia	6,313	Franklin County Public Schools in rural Virginia experienced a ransomware attack, prompting closure on May 15, 2023. The school system, which did not pay a ransom, swiftly addressed the issue, and classes resumed on May 16.
Pineland Regional Schools, New Jersey	1,621	On April 17, 2023, LockBit claimed possession of 64GB of data, intending to release it on April 18. The evidence included a directory image suggesting a substantial amount of personal information, totaling 233GB, potentially impacting both students and personnel. The ransom demand amount from LockBit was not disclosed in their listing.

A LESSON PLAN FOR K12 CYBERSECURITY

Securing K-12 networks from attack can seem like a daunting task. But there are steps that organizations of all sizes can implement. Here are four actions that every school and district should be taking.

Implement Core Cybersecurity Protections

Core steps that every district should take include sanitizing all traffic to and from the Internet by filtering out malware and blocking access to malicious documents; restricting who has access to administrative protocols; implementing multi-factor authentication (MFA) and improving password management; and performing regular maintenance by installing security updates, backing up critical systems, and ensuring that sensitive data is protected, archived, and deleted when no longer needed.

Monitor Systems 24-7

Because cyber criminals are always active, you need to be watching your IT systems at all hours. Not only will this help you protect your systems, but if a breach does occur, you'll be in a better position to respond, contain the breach, and minimize the damage, as time is of the essence during an attack.

Start with the Right Tools

In securing school districts, prioritizing the right tools is paramount to mitigating sophisticated threats. Begin with robust Endpoint Detection and Response (EDR) systems for real-time threat monitoring and automatic responses. Enhance network defenses with Next-Gen Firewalls to block complex attacks, ensuring safe internet access. Strengthen email security through anti-phishing measures and Data Loss Prevention (DLP) to safeguard against cyber threats, protecting students and staff from data breaches.

K12 CYBERSECURITY BY THE NUMBERS

89%
Increase

in ransomware attacks on schools from 2022 to 2023.

$53
Billion

in costs from ransomware attacks in education over the last five years.

11.6
Days

in average downtime from a ransomware attack in 2023 (up from 7.9 days the prior year).

66%
of School Districts

don't have a full-time cybersecurity employee.

68%
of district IT Leaders

say they don't have enough cybersecurity resources to combat risks or aren't sure.

Consider Partnering with a Trusted Provider for Help

While many K-12 districts lack the expertise on staff to implement sophisticated cybersecurity systems, a reliable service provider with experience in serving K-12 education can help.

The hard truth is that *no* school or district will be able to protect their systems against an attack without the right cybersecurity tools in place. No amount of preventive work or training is sufficient by itself, because cyber criminals are smart, sophisticated, and are using AI faster than organizations can adapt. Schools and districts must move beyond firewalls and user training to protect student data, using tools that are as sophisticated as the attacks they are designed to confront. What's needed are proactive detection and response technologies that use AI to swiftly identify anomalies and respond automatically. With these tools, even if teachers or students click on a link they shouldn't, the attack can generally be stopped.

For instance, ActZero delivers a powerful and affordable full-stack cybersecurity service to protect K-12 institutions against ransomware attacks. We bring deep expertise—from the White House, CIA, and Department of Defense—in defense of your IT systems. We track the latest techniques of sophisticated cyber attackers and stop them quickly.

Our proprietary AI enables us to stop threats four times faster than traditional defenses, uncovering advanced cyberattacks missed by most security solutions. We've automated most of the manual work to stop threats across endpoints, mobile devices, network, email, cloud, and identity systems within 15 minutes. Combining this AI with our 24/7 Security

Operations Center staff expertise, we block fast-moving ransomware attacks, continuously filter out false positives and white noise, perform threat hunting daily, and escalate only critical alerts.

ActZero also gives schools and districts complete visibility into vulnerabilities, compliance requirements, executive reporting, and live staff support 24-7 from our customer experience team. This is a complete package to take care of cyber defense requirements, meet compliance rules, qualify for cyber insurance, and keep your school district safe.

ActZero
a WatchGuard brand

San Francisco / Seattle / Toronto / Dublin / Manila
info@actzero.com
actzero.ai
+1-855-917-4981