K-12 Cyberthreat Brief 2025

Lumu Technologies

INTRODUCTION

Cyberattacks against K-12 school districts are escalating, posing a significant threat to educational continuity and the safety of sensitive information. **These incidents directly disrupt learning environments, compromise confidential student and staff data, and strain already limited resources.** K-12 institutions face the unique challenge of safeguarding a vulnerable population and critical infrastructure, often without the cybersecurity budgets or specialized staff common in other sectors.

This report provides K-12 leaders and IT professionals with a concise snapshot of the current cyberthreat landscape impacting schools, its tangible consequences, and essential measures to bolster defenses and protect the learning mission.

THE K-12 THREAT IN NUMBERS (LATEST FIGURES)

Recent data paints a stark picture of the cyber risks facing K-12 schools today. It's clear these aren't isolated incidents, but a widespread challenge impacting the vast majority of educational institutions. Here are some key figures from late 2024 and early 2025:

- **Overall Cyber Threat:** A significant 82% of K-12 schools experienced cyber threat impacts between July 2023 and December 2024 . This included 9,300 confirmed cybersecurity incidents across approximately 5,000 institutions.
- **Ransomware Attacks:** In 2024, a total of 116 K-12 school districts in the U.S. reported ransomware incidents. These attacks impacted an estimated 2,275 K-12 schools, averaging nearly 20 schools per incident. This represents an increase from the 108 incidents affecting K-12 school districts in 2023.
- **Learning Disruption:** 67% of school districts affected by cyberattacks experienced a loss of access to student records for more than five days. The average recovery time for a school district after a cyberattack is around 23 days. Cyberattacks can lead to disruptions in school meal services, forced school closures, and blocked access to crucial student services like special education and counseling .
- **Financial Costs:** The mean cost for K-12 organizations to recover from a ransomware attack in 2024 was $3.76 million, more than double the $1.59 million in 2023.
- **Data Breach Impact:** A December 2024 cyberattack on PowerSchool compromised the personal data of 62.4 million students. Another December 2024 breach at Carruth Compliance Consulting impacted over 40,000 school employees at approximately 36 school districts, exposing sensitive information like Social Security numbers and financial data.

NOTABLE RECENT K-12 CYBERSECURITY INCIDENTS

Alabama State Department of Education (June 2024): The department experienced a ransomware attack where some data was infiltrated. Officials stated they did not pay the ransom.

Granite School District (2024): This Utah school district was targeted by a ransomware attack with a demand of $1.5 million. It is unknown if the ransom was paid.

Freehold Township School District (Early 2024): A ransomware attack on this New Jersey school district was severe enough to cause the cancellation of classes.

ANALYSIS: WHY K-12 AND WHAT TO DO

The figures clearly show K-12 schools are in the crosshairs. Understanding why, and knowing the essential first steps for defense, is crucial.

Why K-12 is Targeted

- **A Treasure Trove of Data:** Schools hold vast amounts of sensitive student PII (protected by FERPA) and staff data, which is valuable to cybercriminals for fraud or extortion. Students often have clean credit histories and may not check their credit rating until after they leave school, giving cybercriminals a number of years with which to monetize students' identities.
- **Operational Pressure:** Attackers know schools are essential community hubs and cannot afford lengthy disruptions to learning, increasing pressure to potentially pay ransoms or resolve issues quickly.
- **Resource vs. Complexity Gaps:** K-12 often operates with limited cybersecurity budgets and specialized staff, while managing large, complex networks with diverse users (students, staff, guests) and numerous devices (including BYOD).

Essential Defenses for K-12: While comprehensive security is complex, focusing on high-impact areas is key for resource-constrained schools

- **Enhance Network Visibility:** You can't protect what you can't see. Implementing tools to monitor network activity helps detect compromises before they cause major disruption, minimizing lost learning time.
- **Automate Detection & Response:** Leverage cost-effective technologies that automatically identify threats and can initiate responses. This acts as a force multiplier, helping limited IT staff manage threats more efficiently.
- **Don't Disregard the Summer or Holiday Breaks:** The Summer, end-of-year period presents a window of opportunity for cybercrime when IT staff are either on leave or otherwise occupied to get ready for the new year. Many organizations lower their guard or delay the deployment of defense technology when we should do the opposite.
- **Master Foundational Hygiene:** Consistently patching software vulnerabilities, enforcing Multi-Factor Authentication (MFA) wherever possible, and ensuring reliable data backups are fundamental, high-impact steps that thwart many common attacks. For more on the basics, consult CISA's guide for schools.

CONCLUSION: SECURING OUR SCHOOLS

The cybersecurity threat to K-12 education is significant, immediate, and constantly evolving. The potential disruption to learning and the compromise of sensitive data demand urgent attention. While the challenges faced by schools are unique, focused, proactive steps can significantly strengthen defenses. Prioritizing foundational security measures, enhancing visibility into network activity, and leveraging automation are critical starting points for protecting students and staff. We encourage all K-12 leaders and IT professionals to assess their current security posture and prioritize these essential actions today. Learn more at lumu.io/cybersecurity-for-schools

Lumu Technologies Inc. | 8600 NW 36th St., Suite 150 Doral, FL 33166 | sales@lumu.io | +1 (877) 909-5868