

Finding Ways to Solve the Cybersecurity Challenge

Federal agencies lend their support to K–12 schools.

MORE THAN 2.6 MILLION STUDENTS ACROSS the United States were affected by ransomware attacks alone from 2018 to 2021, the U.S. **Government Accountability Office (GAO) reports**. Factoring in other kinds of incidents, the total number of students impacted by cybersecurity breaches during that time is even larger.

As malicious threat actors increase their attacks on K–12 networks, with “potentially catastrophic” effects on educators, students, and their families, U.S. government agencies such as the GAO and the Cybersecurity and Infrastructure Security Agency (CISA) are stepping up to help schools and districts secure their cyber infrastructure.

The assistance comes at the request of Congress,

which enacted the K–12 Cybersecurity Act of 2021 to protect K–12 institutions from cyberattacks.

Network security breaches have resulted in lost money and instructional time for schools from coast to coast. K–12 officials who’ve experienced a cyberattack reported that the loss of learning ranged anywhere from three days to three weeks and the recovery time ranged from two to nine months, the GAO says.

In an October 2022 report, the GAO recommended that the U.S. Department of Education develop metrics for measuring the effectiveness of K–12 cybersecurity products and services, as well as a way to coordinate cybersecurity efforts between schools and various federal agencies.

Recommendations

CISA published **its own report** in January 2023, with cybersecurity recommendations for schools and districts. CISA's suggestions include:

Focus on high-impact strategies first.

Because K–12 school systems often have limited resources, leaders should “leverage security investments to focus on the most impactful steps” initially, CISA says, prioritizing strategies such as deploying multi-factor authentication (MFA), mitigating known exploited vulnerabilities, implementing and testing data backups, creating an incident response plan and launching a comprehensive cybersecurity training program.

Once leaders have taken these steps, they can progress to other measures, such as fully adopting CISA's **Cybersecurity Performance Goals** and building a cybersecurity plan around the National Institute of Standards and Technology (NIST) **Cybersecurity Framework**.

Elevate cybersecurity as a top priority.

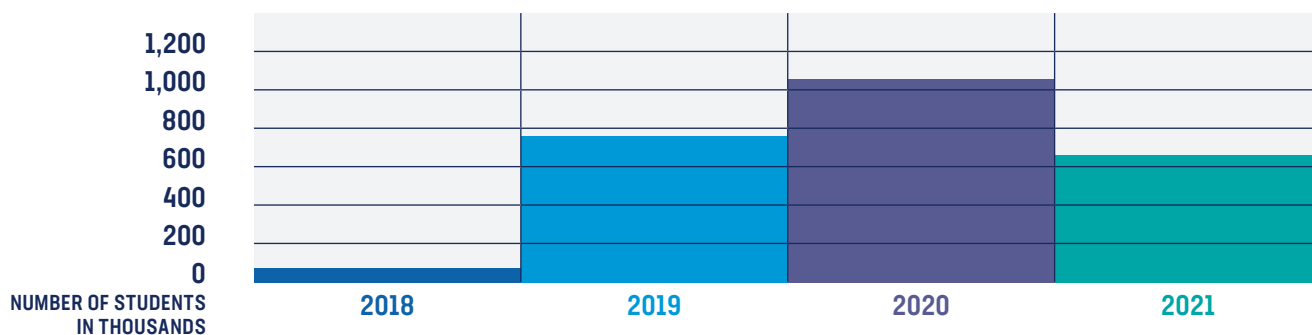
Cybersecurity risk management must become a top priority for the leaders in every K–12 district, CISA says. Leaders must take creative approaches to securing the necessary resources to make this happen.

Superintendents and school boards are critical to these efforts. “Change must come from the top down,” the organization notes. “Leaders must establish and reinforce a cybersecure culture. Information technology and cybersecurity personnel cannot bear the burden alone.”

Collaborate with other partners.

“No K–12 institution is an island,” CISA writes. “Information sharing and collaboration with peers and partners is essential to build awareness and sustain resilience.” K–12 districts should participate in information sharing forums such as the **K12 Security Information Exchange** (K12 SIX) and establish relationships with CISA and FBI field personnel, among other entities.

NUMBER OF U.S. STUDENTS AFFECTED BY RANSOMWARE ATTACKS, 2018-21



Source: GAO analysis of Comperitech study on K–12 school ransomware attacks. | GAO-23-105480

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.