

CyberEDU

Carahsoft Vertical Overview

Summary:

Cybersecurity has become a predominant topic within the education systems as adversaries continue to target K-12 schools and higher education. The programs and initiatives outlined in this overview aim to advance cybersecurity within educational institutions, as cyberattacks can lead to school closures, compromise personal and financial information, and result in data breaches. Collaboration between the federal government, private sectors, academia, and state and local government is essential to foster the requirements of a cyber-resistant education system.

Overview

The modern world relies heavily on information technology for many of its operations, and U.S. schools are no exception. Whether its K-12 or higher education, schools incorporate technology at almost every level, from inputting personal and financial information of staff and students to maintaining online learning platforms. The United States has over 128,000 [K-12 schools](#) and 11,000 [higher education](#) institutions. These educational institutions are one of the sixteen critical infrastructure sectors and include both government and private sector facilities. This highlights the importance of educational institutions to the nation's security, economy, and overall well-being.

Digital services, such as responsive websites and apps, play a crucial role in education by providing students with access to class schedules, campus offerings, grades, and forms. The Department of Education (DOEd) serves as the education systems Sector Risk Management Agency (SRMA), ensuring the safety and implementation of legislation for these institutions. The education subsector includes K-12, higher education institutions, and business and trade schools, all of which contribute significantly to the nation's educational landscape.



"The continued impact of cyber intrusions is threatening the nation's ability to educate our children while also placing personal information and school data at risk. We can, and we must, do better for our nation's youngest learners."

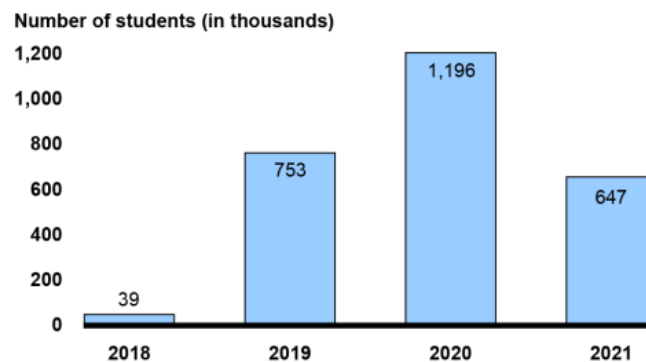
Alaina Clark, Assistant Director for Stakeholder Engagement, CISA

Often, networks and systems at schools are interconnected with internal and external enterprises, making them susceptible to threat actors. The aim of cyberattacks on education are financial gain, disrupting classes, or other potentially destructive objectives. Implementing a cybersecurity strategy to mitigate exposure and improve

security is crucial to protect against digital threats. Investing in cybersecurity before an attack can save school districts money as the monetary loss after a cyber incident range from \$50,000 to \$1 million.

Trends

Covid-19 forced educational institutions across the nation to become virtual which amplified institutions' vulnerability to threats. Enhancing cybersecurity resiliency became essential as ransomware and cyberattacks on educational institutions began to rise. Investing in cyber solutions early can save schools money compared to being vulnerable and having to recover from an attack. The figure showcases the number of students in the United States that are affected by ransomware attacks within K-12 schools.



[GAO Report](#) on K-12 Cybersecurity

Cyberattacks can cause monetary losses due to time and resources needed to recover. A cyber or ransomware attack on a school can lead to disruptions in student learning, compromise security, and substantial financial loss. The time of learning lost after a cyberattack ranges from 3 days to 3 weeks, and the recovery time ranges from 2 to 9 months. K-12 schools need to better address their cybersecurity needs, and the [GAO](#) has advised that the Department of Education (DoEd) and Cybersecurity and Infrastructure Security Agency (CISA) measure the effectiveness of cyber protection products.

Solutions

The GAO found the most common type of cyberattacks in K-12 were phishing, ransomware, denial of services (DoS), and video conferencing disruptions. To combat cyber threats, it is [advised](#) educational institutions should build cyber resiliency by implementing multifactor authentication, cyber awareness, web application firewall, proper software updates, cyber incident response plan, and end-to-end encryption. Investing in cyber solutions and raising staff and student awareness will minimize vulnerabilities, save schools time, and funds.

Initiatives

States and local governments hold the primary responsibility of education as they develop curriculum, give funding, and set requirements. The federal government does however play a significant role within education as it sets policy recommendations, provides resources, and conditional funding. As a result of eight K-12 school districts having significant cyberattacks in the 2022-2023 academic year, the Biden-Harris Administration launched an effort to enhance cybersecurity in K-12 schools. The [initiative](#) lists resources, best practices, and additional cyber funding. In 2023, Cisa is revealed the [Protecting Our Future: Partnering to Safeguard K-12 organizations from Cybersecurity Threats](#). This toolkit provides resources and guidance for K-12 schools to enhance their cyber resiliency. The

Department of Education has stated that the [NIST Cybersecurity Framework](#) should be used within educational institutions to establish proper cybersecurity risk management.

Top Funding

K-12 schools receive funding through local, state, and federal funds. Public schools have the highest budget but are often restricted on spending. Higher education entities have additional revenue sources from traditional state and local governments (tuition, donors, athletics). Listed below are some of the top IT funding sources for education.

- [American Rescue Plan](#) (ARP) - Higher Education Emergency Relief Fund **\$89.5B**. Obligated by end of 2024 and spent by 2026.
- [E-Rate Program](#)- The program currently has a commission established cap of **\$4.456B** and can be adjusted annually. Provides funding for schools and libraries to purchase discounted internet, data transmission services, and services which handles managing internal networks and internal connections.
- [Cybersecurity Pilot Program](#)- Provides up to **\$200M** over a three-year term for cybersecurity services and equipment. Schools and libraries must meet the E-Rate program's eligibility requirements as this is an expansion of the E-Rate program.

The school districts with the highest budgets and estimated IT budgets are outlined below with the top jurisdiction being New York City Public Schools.

Jurisdiction Name	Level	Total Budget	Estimated IT Budget
New York City Public Schools	Public School District	\$38,000,000,000	\$760,000,000
Los Angeles Unified School District	Public School District	\$13,800,000,000	\$280,000,000
Chicago Public Schools	Public School District	\$7,820,000,000	\$160,000,000
Clark County School District	Public School District	\$6,886,093,424	\$140,000,000
Orange County Public Schools	Public School District	\$5,233,059,938	\$100,000,000
Broward County Public Schools	Public School District	\$4,751,445,938	\$95,000,000
School District of Palm Beach County	Public School District	\$3,822,756,506	\$76,000,000
Miami-Dade County Public Schools	Public School District	\$3,674,871,190	\$73,000,000
School District of Philadelphia	Public School District	\$3,401,866,211	\$68,000,000
Fairfax County Public Schools	Public School District	\$3,378,618,144	\$68,000,000

Higher education schools with the highest estimated IT budgets are outlined below with the top institution being University of California-Los Angeles.

Jurisdiction Name	Estimated IT Budget
University of California-Los Angeles	\$366,808,360
University of California-San Francisco	\$325,738,920
Stanford University	\$308,344,000
University of California-Davis	\$276,000,000
University of California-San Diego	\$252,668,000
Cornell University	\$227,639,720
Columbia University in the City of New York	\$218,475,600
Weill Cornell Medical College	\$199,462,840
University of Rochester	\$197,482,840
University of Florida	\$191,596,555
New York University (NYU)	\$158,280,000
University of Texas Southwestern Medical Center	\$140,000,000
University of Texas at Austin	\$140,000,000
University of Texas Medical Branch	\$110,000,000
University of South Florida-Tampa	\$93,596,510
Texas A & M University-College Station	\$86,000,000
Baylor College of Medicine	\$84,000,000
University of Central Florida	\$78,791,113
Florida State University	\$72,416,190
Florida International University	\$68,928,000
Grand Total	\$3,596,228,648