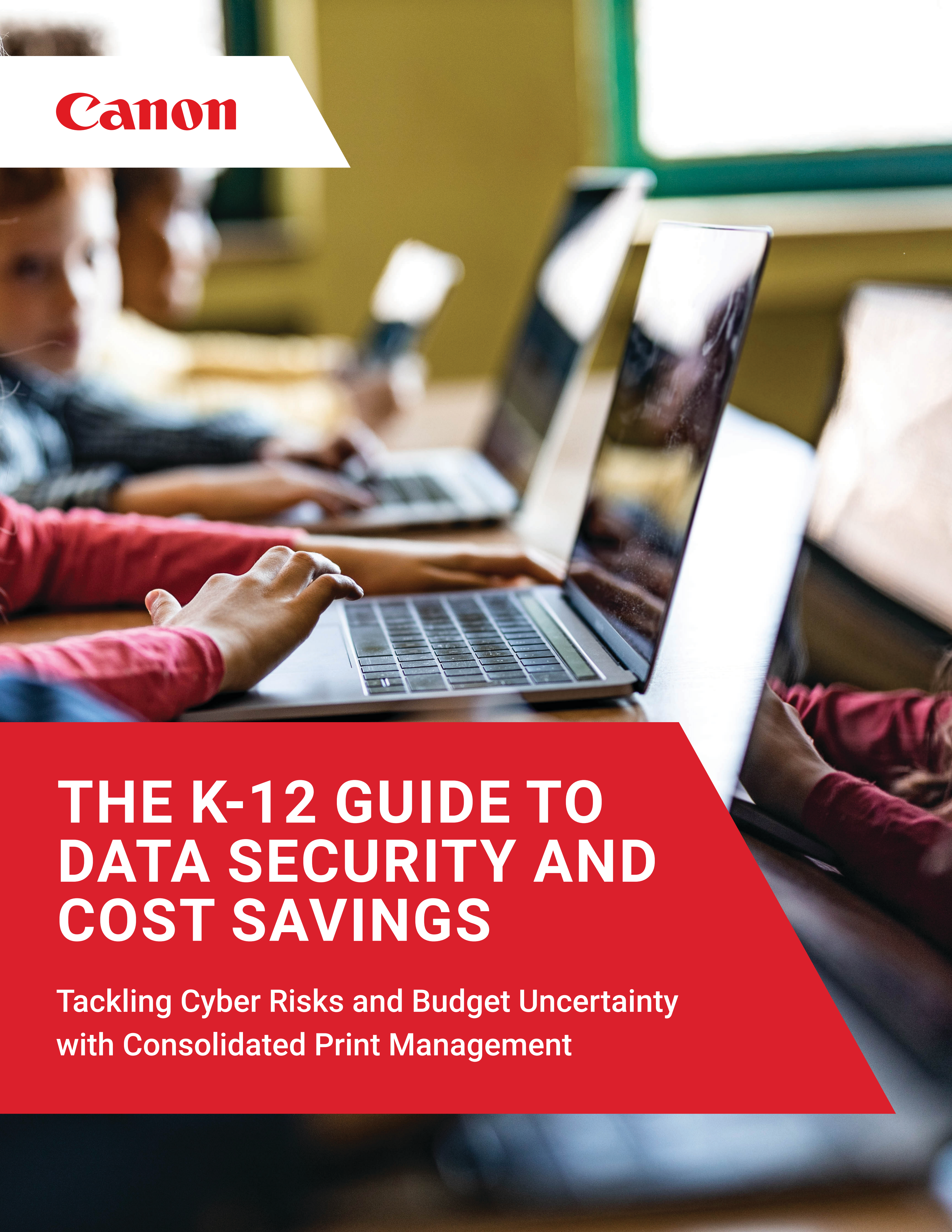


THE K-12 GUIDE TO DATA SECURITY AND COST SAVINGS

Tackling Cyber Risks and Budget Uncertainty with Consolidated Print Management

FLAT BUDGETS, ESCALATING RISKS

Reduced funding from federal and state governments puts cybersecurity at risk inside K-12 schools. Yet a single cyber incident can become one of the largest unplanned expenses for any district. The core challenge for administrators and IT teams: How to reduce security risks while stretching limited funds?

81%
of K-12 districts say insufficient funding is their top security concern.[1]

A single ransomware attack can cost
nearly $1 million.[2]

Budgets and IT Teams Get Smaller

School districts cannot carry over unused IT dollars into the next year, forcing difficult spending choices. Simultaneously, inflation and the expiration of federal Elementary and Secondary School Emergency Relief (ESSER) funds mean that K-12 funding will remain flat through 2028.[3]

Staffing shortages add pressure. Experienced IT leaders are retiring. Highly skilled technicians are leaving, lured away to the private sector by larger salaries.

$21 billion
gap between spending and funding.[4]

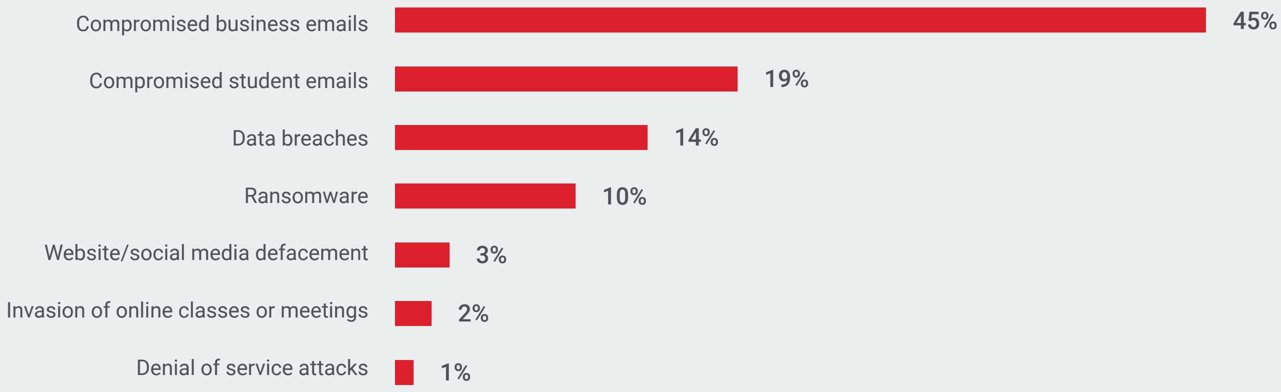
Cyber Threats Loom Larger

Districts face continuous cyber threats, from phishing to financial fraud.

- The average district experiences **five** cyber incidents per week.[5]
- Yet while **59%** worry about the increasing sophistication of threats, **58%** lack documented cybersecurity processes.[6]

To help save money and strengthen security, districts need a clear view of where risks and hidden costs actually live.

Top Cyber Threats in K-12[7]



HELP SECURE THE WEAKEST LINKS

Budget savings and cyber threats share a common trait: they both hide in plain sight.

Fragmented IT Breaks Budgets

One of the most overlooked cost drains is the patchwork of printers, scanners, copiers, and multifunction devices (MFDs) that schools rely on to create essential documents—everything from parent newsletters and report cards to diplomas and student achievement awards. Here's how the costs add up.

- **Multiple leases signed at the school level** = Inconsistent pricing and redundant payments
- **Multiple contracts with varying end dates** = No leverage for volume discounts
- **No visibility into device usage** = Unnecessary spend on paper and supplies
- **Higher burden on IT staff** = Time spent "fixing" disparate devices and systems

Human Vulnerabilities Create Breaches

Nearly half of K-12 incidents stem from human error.[8] One school district lost $1.3 million—and recovered only 85% of the costs—after a phishing attack.[8] Other preventable breaches occur when:

→ **Legacy technology** lacks modern security protocols.

→ **Printed student records** are left unattended by a printer.

Cyber Insurance: The Good (and the Bad)

Cyber premiums keep rising, with some districts reporting increases of up to 70% over the last three years.[8] Most carriers now require proof of cyber hygiene, such as end-user training or multi-factor authentication (MFA), before writing policies.

STRONG SECURITY SAVES MONEY

The best defense against cyberattacks is an informed staff. Leading districts are fortifying their "human firewall" by committing to continuous training.

30% cost savings

and double coverage for one district that embraced end-user training, MFA, and monitoring tools.[8]

Implement phishing simulations and MFA

Mirror real-world threats and require mandatory retraining for all staff who fail. MFA necessitates two forms of identification (such as a password and a badge swipe) to access hardware and software.

Give students a role in cybersecurity

Some K-12 schools are implementing AI, cybersecurity, and digital literacy training into their curriculum. Doing so helps protect the district's networks and prepares pupils for future careers.

Consider a set of "outside eyes"

Districts increasingly rely on third parties to conduct external risk assessments. Another popular option: managed IT partnerships that offer access to expertise districts cannot hire internally.

Know the latest standards

Trusted organizations publish in-depth guidance tailored for K-12:

- **Cybersecurity & Infrastructure Security Agency (CISA):** Tools, resources, and recommendations to help schools mitigate cyber threats
- **K-12 Security Information eXchange (K12 SIX):** Threat intelligence and best practices for preventing and responding to cyber threats

Crack the code. Discover more best cybersecurity practices in EnvisionED K-12 magazine.

Learn more.

SIMPLIFY THE PRINT FLEET

A secure, end-to-end, cloud-based print and scan workflow is within reach for most districts. With limited funds, administrators, IT, and procurement teams should invest early and wisely. Seek superintendent and board buy-in and prioritize long-term projects over quick fixes. **Consolidating your print fleet can help deliver significant benefits:**

Cost savings: Replacing multiple desktop printers with network-connected multifunction devices (MFDs) can help reduce supply and energy consumption.

Contract predictability: Consolidating all devices under one license with cost-per-copy billing can create easier budgeting and consistent renewal cycles.

Automated workflows: Cloud-based solutions can integrate seamlessly with existing IT infrastructure, so districts can reduce labor costs by digitizing enrollment packets and student record requests.

Multiple authentication methods: Best-in-class devices like imageFORCE from Canon require users to be standing at the printer to release a job. Users authenticate using a badge swipe, username, password, PIN code, or job code.

Centralize print management: Canon's uniFLOW online provides control over Canon and non-Canon printer fleets, supporting multi-vendor environments.

Track and audit print costs: Optimize paper usage, save on ink, and reduce outsourcing for high-volume printer needs.

Canon's print and document ecosystem aligns with CISA and K-12 SIX guidelines, helping districts to strengthen security and reduce costs simultaneously.

Explore how Canon can help enhance education for K-12.

SOURCES:

[1] CoSN, "New Report Details K-12 Schools' Top Cybersecurity Concerns," November 2023.
[2] Sophos News, "K-12 schools face cybersecurity risks inside and outside of the classroom," September 2025.
[3] Center for American Progress, "The Sudden Loss of Federal COVID-19 Relief Funds Will Hinder K-12 Academic Progress," May 2025.
[4] Education Data Initiative, "U.S. Public Education Spending Statistics," February 2025.
[5] U.S. Department of Education, "K-12 Cybersecurity: School Safety and Security," September 2025.
[6] CoSN, "New Report Details K-12 Schools' Top Cybersecurity Concerns," November 2023.
[7] RAND Corporation, "Protecting Schools Virtually: Cybersecurity and Threats on K–12 School Computer Systems," September 2025.
[8] Canon Q4 2025 K-12 Education Advisory Board Meeting.

Canon

1-844-50-CANON
USA.CANON.COM/BUSINESS

Canon USA does not provide legal counsel or regulatory compliance consultancy, including without limitation, regarding Sarbanes-Oxley, HIPAA, CCPA, GDPR, GLBA, Check 21, or the USA Patriot Act. Each customer must have its own qualified counsel determine the advisability of a particular solution as it relates to regulatory and statutory compliance. Canon products offer certain security features, yet many variables can impact the security of your devices and data. Canon does not warrant that use of its features will prevent security issues. Some security features may impact functionality/performance; you may want to test these settings in your environment.