PROTECTING OUR FUTURE:

PARTNERING TO SAFEGUARD K–12 ORGANIZATIONS FROM CYBERSECURITY THREATS

PUBLICATION: JANUARY 2023

U.S. DEPARTMENT OF HOMELAND SECURITY
CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

TABLE OF CONTENTS

02 **Executive Summary**

04 **Introduction**

06 **Risks and Challenges to the K–12 Education Community**

08 **FEEDBACK FROM STAKEHOLDER ENGAGEMENT**

08 RESOURCE | Shortage of Cybersecurity Professionals in K-12 Institutions

09 SIMPLIFY | Desire for Clear, Actionable Guidance and Cybersecurity Plans for Ready Adoption

09 PRIORITIZE | Role for Centralized Governance in Planning and Advising on Resource Allocation

10 GOVERN | More Effective Oversight and Accountability

11 **RECOMMENDATIONS**

12 Key Findings and Recommendations

13 **Recommendation 1.** Invest in Most Impactful Security Measures and Build Toward a Mature Cybersecurity Plan

16 **Recommendation 2.** Focus on Collaboration and Information Sharing

18 **Recommendation 3.** Recognize and Actively Address Resource Constraints

19 **Conclusion**

20 **Acknowledgements**

21 **Appendix 1. K–12 Resource Repository**

23 **Appendix 2. Key Resources**

27 **Footnotes**

IMPLEMENT MOST IMPACTFUL **SECURITY MEASURES**

FIRST

1. Implement multifactor authentication [MFA]
2. Prioritize patch management
3. Perform and test backups
4. Minimize exposure to common attacks
5. Develop and exercise a cyber incident response plan
6. Create a training and awareness campaign at all levels

SECOND

Prioritize further near-term investments in alignment with the full list of CISA's Cybersecurity Performance Goals [CPGs]

THIRD

Develop a unique cybersecurity plan that leverages the NIST Cybersecurity Framework [CSF]

EXECUTIVE SUMMARY

There is no more important institution to the future prosperity and strength of the United States than our nation's K–12 education system. K–12 schools and school districts have adopted advanced networking technologies that facilitate learning and make schools more efficient and effective. This technological gain, however, has introduced heightened risks. Malicious cyber actors are targeting K–12 education organizations across the country, with potentially catastrophic impacts on students, their families, teachers, and administrators.

The K–12 cybersecurity challenge was exacerbated by the COVID-19 pandemic, which significantly tested the nation's education system, necessitating an unexpected pivot to virtual learning that rendered our K–12 educational institutions increasingly vulnerable as new technologies were adopted on an unprecedented scale. Cyberattacks, and the threat thereof, strained resources and impacted delivery of critical education services across the nation. This has placed an untenable burden on our educational institutions and the populations that they serve and protect—children, parents, and educators. A continuing drumbeat of cyber intrusions is threatening the nation's ability to educate our children while also placing personal information and school data at risk.

Congress recognized this heightened risk environment by enacting the K–12 Cybersecurity Act of 2021 ("The Act"), which required the Cybersecurity and Infrastructure Security Agency (CISA) to report on cybersecurity risks facing elementary and secondary schools and develop recommendations that include cybersecurity guidelines designed to help schools face these risks. Our resultant report provides insight into the current threat landscape and the K–12 community's capacity to prevent and mitigate cyber attacks. Recommendations throughout this report are informed by insights from policy-makers, government officials, and members of the K–12 community. These recommendations are presented with a caveat: **change must come from the top down**. Leaders must establish and reinforce a cybersecure culture. Information technology and cybersecurity personnel cannot bear the burden alone.

This report is only a starting point. CISA will continue to engage with federal partners, including the U.S. Department of Education, and work closely with state and local officials, school leaders, emergency management officials, nonprofits, community leaders, and the private sector to identify areas for progress and provide meaningful support that measurably reduces risk.

INTENDED AUDIENCE

This report is principally intended for leaders in the K–12 community, including superintendents, district and school administrators, school boards, and state policymakers. The report may also be useful for education and technology leaders, including cybersecurity and IT staff, federal agencies, non-federal cybersecurity entities, nonprofits, and private sector organizations supporting the K–12 community. It is intended to raise awareness of the K–12 community's growing cyber risk and threat landscape and catalyze action across the K–12 community.

KEY FINDINGS

01

In an environment of limited resources, leaders should leverage security investments to focus on the most impactful steps. K–12 entities should begin with a small number of prioritized investments: deploying multi-factor authentication (MFA), mitigating known exploited vulnerabilities, implementing and testing backups, regularly exercising an incident response plan, and implementing a strong cybersecurity training program. K–12 entities should then progress to fully adopting CISA's Cybersecurity Performance Goals (CPGs) and mature to building an enterprise cyber-security plan aligned around the NIST Cybersecurity Framework (CSF).

02

Cybersecurity risk management must be elevated as a top priority for administrators, superintendents, and other leaders at every K–12 institution. Leaders must take creative approaches to securing necessary resources, including leveraging available grant programs, working with technology providers to benefit from low-cost services and products that are secure by design and default, and urgently reducing the security burden by migrating to secure cloud environments and trusted managed services.

03

No K–12 institution is an island. Information sharing and collaboration with peers and partners is essential to build awareness and sustain resilience. K–12 entities should participate in an information sharing forum such as the Multi-State Information Sharing and Analysis Center (MS-ISAC) and/or K12 Security Information eXchange (K12 SIX) and establish a relationship with CISA and FBI field personnel.

INTRODUCTION

As the nation's cyber defense agency, CISA has supported the K–12 education community in responding to and managing an increasing number of cybersecurity incidents, including by serving as a conduit for operational information sharing and guidance. In recent years, the cybersecurity challenge facing the K–12 community has only grown. The COVID-19 pandemic forced schools to pivot toward more virtual learning and quickly provide new technology, such as laptops or tablets, to students, teachers, and other faculty. Even as the worst days of the pandemic threat have subsided, K–12 institutions have recognized the broader benefits of these innovations and permanently changed operational practices accordingly. Threat actors, who were already escalating their attacks on K–12 institutions prior to the pandemic, have taken advantage of the increased post-pandemic attack surface and dependence on networked technologies to target K–12 institutions, often with disruptive or damaging results.

Increasingly, school or school district systems have been breached, with data deleted, misused, or even held for ransom. This trend has continued throughout 2022, and leaders across the K–12 community are coming to recognize that no school, district, or organization is immune from cyber intrusions. Low-income districts are in many cases most at-risk and vulnerable to cyberattacks and need focused support given lack of financial resources.[1]

The K–12 Cybersecurity Act of 2021 directed CISA to study cybersecurity risks facing elementary and secondary schools, develop voluntary recommendations, including cybersecurity guidelines, and evaluate challenges that schools face in securing information systems owned, leased, or relied upon by K–12 educational institutions. Further, the Act required CISA to **(1)** develop an online training toolkit designed for school officials; and **(2)** make available the study's findings, cybersecurity voluntary recommendations, and the toolkit. The Act also required CISA to consult with cybersecurity and education entities, including teachers, school administrators, federal agencies, non-federal cybersecurity entities with experience in education issues, and private sector organizations.

To fulfill the Act's requirement for stakeholder input, CISA hosted and facilitated a series of roundtable listening and feedback sessions with key stakeholder groups outlined in the legislation and relevant to the K–12 education community, including superintendents, principals, school administrators, and teachers. CISA also engaged various partners through individual interviews, meetings, and focused discussions. The roundtable feedback sessions allowed CISA to gain insights into cybersecurity challenges facing the K–12 community and served as a forum to solicit input on proposed key themes, concepts, and areas of focus. Roundtable

topics included **1)** securing information systems owned, leased, or relied upon by K–12 educational institutions; **2)** securing sensitive student and employee records; and **3)** implementing cybersecurity protocols. An overwhelming majority of stakeholders across the educator and administrator communities reported that they had too many responsibilities and not enough time or resources to fulfill them. Most reported that the breadth of available cybersecurity information—news coverage, conference panels, webinars, and more—only made matters more complicated.

> **Nearly all reported that they needed simplicity, prioritization, and resources targeted to the unique needs and context of K–12 organizations. This report is intended to be a step forward in addressing this call, including by providing clear recommendations and resources to help K–12 organizations most effectively reduce their continuously evolving cybersecurity risks.[2]**

CISA's engagement with the K–12 cybersecurity community does not stop with publication of this report. Going forward, CISA will continue to partner with the K–12 education community, and work with technology providers to encourage provision of free or low-cost security tools and products that are secure by default and design. Cybersecurity is a continuously evolving challenge. This report is only a first step toward an environment in which our nation's schools are secure and resilient against cyber threats. But we must take this step, and take it in partnership, with a whole-of-nation effort to provide K–12 institutions with the support, resources, and clear guidance needed to make crucial progress.

RISKS AND CHALLENGES TO THE K–12 EDUCATION COMMUNITY

According to the U.S. Department of Education, K–12 institutions serve more than 50 million students in the United States. Although the total number of K–12 cybersecurity incidents is impossible to reliably quantify due to a lack of consolidated data, research from federal and private sector sources shows that cyber threats have continued to escalate. From 2018 to the present, schools in most states have reported cyber incidents on their systems. Reported incidents between 2018–2021 have risen from 400 in 2018 to an accumulated total of over 1,300. (Figure 1)[3]

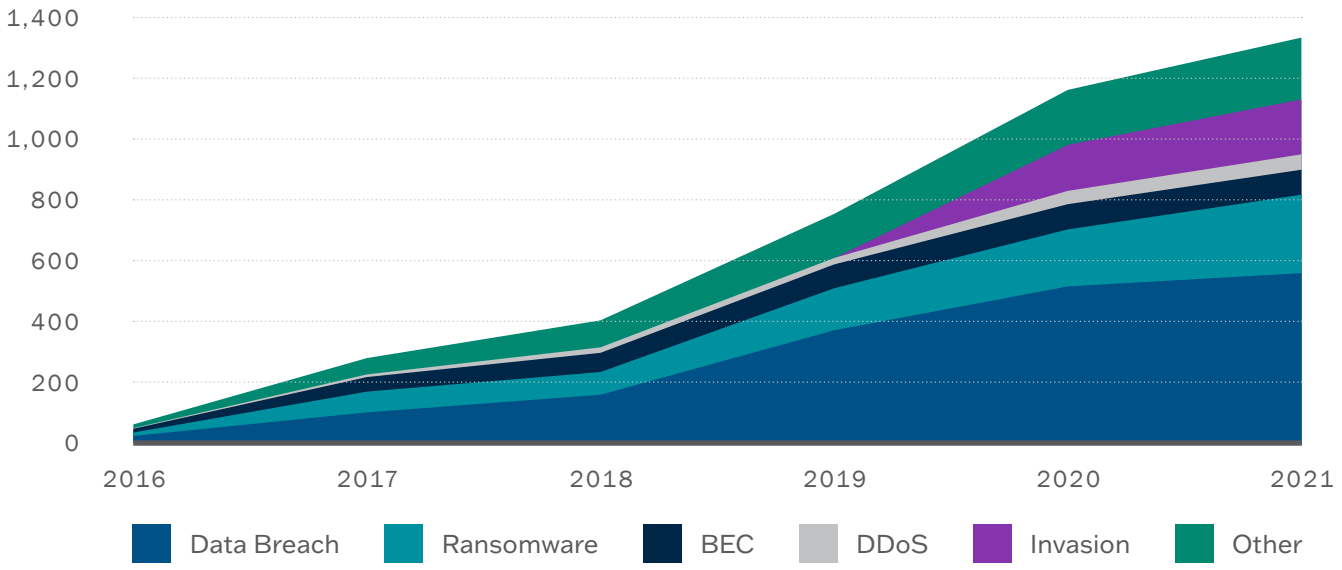

FIGURE 1: NUMBER OF PUBLICLY-DISCLOSED K–12 INCIDENTS BY INCIDENT TYPE: 2016–2021

Malicious cyber actors are targeting school computer systems, disrupting access, and rendering the systems unable to perform basic functions. Moreover, schools, districts, states, and educational technology vendors collect, transmit, and store a range of sensitive information on students and employees including grades, test/assessment scores, addresses, telephone numbers, emails, special education accommodations, disciplinary records, financial information, medical information, and employee Social Security numbers (SSNs). With greater connectivity among these systems and networks, threat actors attack these systems for financial gain, to disrupt classes, or for other potentially destructive purposes.[4] Notwithstanding this continuous onslaught of intrusions, research shows that many school districts lack a chief information security officer (CISO) position and the internal expertise to match the many challenges of cybersecurity today.[5]

According to a recent report by the Multi-State Information Sharing and Analysis Center (MS-ISAC), 29 percent of the ISAC's K–12 school and district members reported being victims of a cyber incident.[6] Types of incidents included:

- Student data breaches
- Data breaches involving information regarding teachers and school community members
- Ransomware attacks
- Business email compromise (BEC) scams
- Denial of service (DDoS) attacks
- Website and social media defacement
- Online class and school meeting invasions

A Government Accountability Office (GAO) report from October of this year found: "From 2018 to the present, schools in most states have reported cyberattacks on their systems. COVID-19 remote learning protocols increased school districts' usage of IT systems and increased the potential for a cyberattack as threat actors view schools as opportunistic targets."[7] More specifically, the report noted cyberattacks on K–12 schools have resulted in:[8]

- **Monetary losses** for targeted schools due to the downtime and resources needed to recover from incidents.
- **Loss of learning** following a cyberattack ranging from three days to three weeks, and full recovery time ranging from two to nine months.
- **Over two million students affected** by ransomware attacks on schools and districts.

Further, data collected by K12 SIX showed that 55 percent of all data breaches at K–12 schools between 2016 and 2021 were carried out on schools' vendors.[9] In January 2022, for example, a ransomware attack on a single vendor of website hosting services took down the websites of 5,000 schools across the country, preventing some of them from sending email notifications about school closures due to COVID-19.[10]

FEEDBACK FROM STAKEHOLDER ENGAGEMENT

Through our engagement efforts, CISA convened numerous stakeholders to gather insights into current topics of concern in the K–12 community. Across the community, educators expressed a need to understand the breadth of threats. School administrators, superintendents, and others in leadership realize that a general awareness of the cyber threat landscape is required to advance strategy, planning, and resourcing. Leaders also highlighted challenges arising from limited resources and staff, and some highlighted benefits that could be achieved through centralization and pooling of resources. Stakeholders across the K–12 community shared key topics of concern, as described below.

RESOURCE

SHORTAGE OF CYBERSECURITY PROFESSIONALS IN K–12 INSTITUTIONS

Many participants in CISA's listening sessions reflected significant resource and staffing challenges. While physical security investments have significantly increased over the last decade, cybersecurity investment lags behind. Leaders expressed a need for increased cybersecurity budgeting and support mechanisms across the community. In particular, participants stressed that funding must be specifically earmarked for cybersecurity; otherwise, hiring a cybersecurity resource will always compete with hiring a teaching resource or other priorities—particularly challenging in a time when overall budgets in many school districts are increasingly strained.

Participants noted that most districts do not employ full-time cybersecurity personnel, and some smaller school districts may not even employ full-time IT staff.[11] Participants further noted that many cybersecurity staff who are currently employed by schools do not have up-to-date training or experience, in part due to limited resources for professional development. If a school is fortunate enough to have a security expert on staff, this individual may not get leadership support to implement critical controls such as multifactor authentication. Participants further observed that many districts experience extreme disparity in talent availability and funding, with a clear divide between larger and smaller districts.

SIMPLIFY

DESIRE FOR CLEAR, ACTIONABLE GUIDANCE & CYBERSECURITY PLANS FOR READY ADOPTION

Lack of resources in turn creates challenges in adoption of cybersecurity practices, deciding on appropriate policies, and broadly implementing a strong baseline of defenses. Participants clearly indicated an interest in using an existing framework instead of reinventing new standards, but the lack of cybersecurity expertise in the K–12 community creates challenges planning for and operationalizing necessary technical controls.

Participants specifically expressed concern about controls that are burdensome to implement or have timelines that do not address urgent risks. Participants also noted that many school IT personnel grapple with constant stress around the need to keep school IT systems operational while at the same time taking steps to prevent potential cyberattacks. Scarce resources and divided attention underscore the importance of streamlining efforts to mature K–12 organizations' resilience. At the same time, participants also stated the need for K–12 organizations to build mature, enterprise cybersecurity programs over time, including a robust cybersecurity plan aligned to the organizations specific risk and technology environment.

PRIORITIZE

ROLE FOR CENTRALIZED GOVERNANCE IN PLANNING AND ADVISING ON RESOURCE ALLOCATION

Participants repeatedly stressed that recommendations around governance should be prioritized. Differences in governance inform how a state CISO, where one exists, understands their role within the K–12 community. Some participants explained that the equities of the K–12 community can be brought to a convening body, with a broad base of representation from state leadership, large and small school district leadership, rural district leadership, and any regional or state-wide independent bodies. Participants also discussed the role that centralization can play in planning and resourcing, observing that while some states already provide centralized assistance, in many cases cybersecurity planning and implementation is the domain of individual districts. Additionally, some participants noted the unique importance of centralizing capabilities such as identity and access management, but further noted challenges in implementation due to issues like rapidly provisioning guest accounts for daily school operations (e.g., onboarding parent volunteers). Participants highlighted that centralization may provide an opportunity for scalable progress and suggested development of cybersecurity plans to assist resource-constrained districts with cybersecurity capabilities, technical solution integrations, and standardized resourcing plans.

GOVERN

MORE EFFECTIVE OVERSIGHT AND ACCOUNTABILITY

Many participants echoed concerns over lack of oversight and accountability for cybersecurity affecting K–12 organizations. Some noted that jurisdiction between the state's cybersecurity agency (or agencies) and state education agency is not well articulated. Participants emphasized a need for strong governance models as a foundational capability upon which all other improvements depend. Participants noted that compliance-based audits do not necessarily drive large-scale change or accountability in cases where systems are overwhelmed and under-resourced, but observed that cyber assessments built around accepted security frameworks were nevertheless often useful to highlighting organizational risks. The important role of insurance companies was recognized in uplifting the cybersecurity risk management practices of K–12 organizations by incentivizing control adoption. However, some participants noted that some frameworks used by insurers were not perceived as fully relevant to the K–12 community.

Lastly, participants expressed significant concern about vendor management and contract accountability. Participants observed a current lack of standards and minimal requirements for K–12 vendors and suppliers, including significant variance in organizations' ability to include robust contract language development and appropriate service level agreements (SLAs) to drive vendors to ensure that best practices and lessons learned are followed throughout the duration of the contract. Further, participants noted that if a school district does not have adequate cyber or IT staff, its ability to verify adherence against an SLA is severely limited. While some states have a procurement entity that evaluates and approves cybersecurity and technology services to broader government entities, this process is not consistent across all states, making it very challenging for K–12 leaders to access services with confidence.

RECOMMENDATIONS

Based on feedback from K–12 stakeholders, CISA offers the following recommendations to help K–12 leaders build, operate, and maintain resilient cybersecurity programs.

KEY FINDINGS
AND RECOMMENDATIONS

01

FINDING	RECOMMENDATION
With finite resources, K–12 institutions can take a small number of steps to significantly reduce cybersecurity risk.	**Invest in the most impactful security measures and build toward a mature cybersecurity plan** by taking these three steps: • Implement highest priority security controls. • Prioritize further near-term investments in alignment with the full list of CISA's Cross-Sector Cybersecurity Performance Goals (CPGs). • Over the long-term, develop a unique cybersecurity plan that leverages the NIST Cybersecurity Framework (CSF).

02

FINDING	RECOMMENDATION
Many school districts struggle with insufficient IT resources and cybersecurity capacity.	**Recognize and actively address resource constraints**: • Work with the state planning committee to leverage the State and Local Cybersecurity Grant Program (SLCGP). • Utilize free or low-cost services to make near-term improvements in resource-constrained environments. • Expect and call for technology providers to enable strong security controls by default for no additional charge. • Minimize the burden of security by migrating IT services to more secure cloud versions.

03

FINDING	RECOMMENDATION
No K–12 entity can singlehandedly identify and prioritize emerging threats, vulnerabilities, and risks.	**Focus on collaboration and information sharing**: • Join relevant collaboration groups, such as MS-ISAC and K12 SIX. • Work with other information-sharing organizations, such as fusion centers, state school safety centers, other state and regional agencies, and associations. • Build a strong and enduring relationship with CISA and FBI regional cybersecurity personnel.

RECOMMENDATION 1:

INVEST IN THE MOST IMPACTFUL SECURITY MEASURES

AND BUILD TOWARD A MATURE CYBERSECURITY PLAN

Cybersecurity is not one size fits all. Schools and their districts have distinct strengths and weaknesses and a wide range of needs. At the same time, there are relatively simple actions that every K–12 organization can take to significantly reduce the risk of a damaging intrusion. To that end, CISA recommends that K–12 entities take a three-step approach, as described below.

FIRST, take a small number of the **highest priority steps**:

1. Implement MFA (Cybersecurity performance goal 1.3). Use MFA,[12] a layered approach to securing online accounts and the data they contain. Even if one factor (such as a user password) becomes compromised, unauthorized users will be unable generally to bypass the second authentication requirement, ultimately stopping them from gaining access to the target accounts. Not all MFA methods provide the same level of protection. Some MFA types are better than others. Phishing-resistant MFA is the standard all leaders should strive for, but any MFA is better than no MFA.[13]

MFA implementation can be challenging. CISA has observed that some organizations have instructed their users to enroll in MFA, but not all users complete that task. There are often MFA gaps for recently onboarded staff and for people who have migrated to a new phone. In addition, the recommended phishing-resistant MFA tools are often available only at an additional cost. Finally, many educational technology applications have their own MFA. Given these challenges, including costs, schools should consider whether their networks might benefit from a comprehensive single sign-on (SSO) solution that centralizes identity and access management (IAM) controls.

Leaders may need to take a phased approach to navigate MFA implementation challenges. While best practices includes implementing MFA wherever possible, some districts who are just starting their MFA journey may first implement MFA on their highest risk systems, such as virtual private networks or student information systems, and high-priority accounts. But it is critical that K–12 institutions complete their MFA journey as quickly as possible. System administrators and all users with elevated privileges should enroll in MFA, preferably phishing-resistant MFA. All K–12 entities should regularly look for accounts that are not protected by MFA and remediate.

2. Fix known security flaws (Cybersecurity Performance Goal 5.1). Many attacks succeed because victims were running vulnerable software when a newer and safer version was available. Keeping systems patched is one of the most cost-effective practices an organization can adopt to enhance its security posture. All K–12 entities should sign up for CISA's free *Vulnerability Scanning*[14] service to receive weekly reports on vulnerabilities accessible via the internet and prioritize fixing vulnerabilities listed in CISA's *Known Exploited Vulnerabilities (KEV) Catalog*.[15]

3. Perform and test backups (Cybersecurity Performance Goal 7.3). Many organizations who have fallen victim to damaging intrusions such as ransomware either had no backups or had incomplete/damaged backups. K–12 entities should back up all key systems regularly, and also regularly test partial and full restoration of data. This practice should be documented in a written plan. Backups should be stored offline and disconnected from the network. As part of the entities' governance program, leaders should request and review evidence of the test restoration tasks and workplans to address any gaps found during the restoration exercise.

4. Minimize exposure to common attacks (Cybersecurity Performance Goals 2.1 and 5.4). Many threat actors find vulnerable targets by scanning the internet for exploitable services. K–12 entities should ensure that IT assets accessible via the internet do not expose frequently exploited services. Any exposed system must have strong compensating controls in place and be reviewed as part of the governance program. CISA's *Stuff off Search*[16] page provides additional guidance on this important step. Because attackers frequently compromise Remote Desktop Protocol (RDP) servers, organizations should have their RDP security plan reviewed by both management and outside experts.

5. Develop and exercise a cyber incident response plan (Cybersecurity Performance Goal 7.2). School and district leaders and administrators need to know how to respond to cyber incidents, including how to recover should adverse events occur. Every K–12 organization should establish and regularly exercise a written incident response plan (IRP), which should define what the organization needs to do before, during, and after an actual or potential security incident. It should include roles and responsibilities for all major activities and be approved by the most senior leader of the K–12 organization. Where possible, organization-level IRPs should be integrated into a district's broader emergency operations plan. Successful teams rehearse their plans. Organizations should test their plans by hosting attack simulation exercises with the personnel identified in their IRP. Sometimes called "tabletop exercises" or "TTXs," these simulations allow teams to prepare for the inevitable security incident during peacetime. The lessons learned from these exercises will allow the organization to update and strengthen their IRP as well as their policies, procedures, and even technologies.

6. Create a training and awareness campaign at all levels (Cybersecurity Performance Goal 4.3). The cybersecurity field is not just about technology; it is also about people. Good training focuses on both awareness and enablement. When people on the front lines see something suspicious, do they know how to report it? Do the people who receive the report know how to act appropriately? Investment in training is just as important as investment in cybersecurity capabilities, tools, and solutions. Staff training at all levels is a prerequisite to progress. While leadership, staff, and student time is limited, initiating positive change and driving cyber awareness at all levels is within reach. Free training resources can be curated and administered to build on current training or fill gaps, such as cybersecurity training provided by CISA through the *Federal Virtual Training Environment (FedVTE)*.[17]

SECOND, prioritize further near-term investments in alignment with the full list of CISA's CPGs,[18] a succinct set of high-priority security outcomes and recommended actions applicable to IT and operational technology environments. By implementing these CPGs, organizations can undertake prioritized and targeted investment to address the most significant cybersecurity risks. Each CPG was selected to **(1)** significantly and directly reduce the risk or impact caused by commonly observed, cross-sector threats and adversary tactics, techniques, and procedures; **(2)** be clear, actionable, and easily definable; and **(3)** be reasonably straightforward and not cost-prohibitive for even small and medium-sized entities to successfully implement. In addition, the CPGs are accompanied by a *CPGs Checklist*[19] that allows organizations to prioritize their utilization of each goal based upon cost, complexity, and impact, making the CPGs uniquely useful for organizations with limited resources. To start, school districts should prioritize high-impact, low-cost CPGs.[20] The CPGs will be regularly refreshed and updated, allowing them to be used as a continuously effective resource to drive prioritized investments against the most significant threats and critical risks. In addition, CISA provides a free CPG Assessment that can be administered as a self-assessment or by regional CISA personnel to help an organization identify and prioritize investments toward adoption of the CPGs.

THIRD, develop a unique cybersecurity plan that leverages the NIST Cybersecurity Framework (CSF)[21] and is tailored around each entity's technology and risk environment to enable continued enterprise maturation and focus awareness, strategy, and resource planning; find gaps; and create opportunities to pool shared resources. CISA's cybersecurity advisors are available to support K–12 entities in developing their cybersecurity plans. The goal of this cybersecurity plan should be to define a target maturity state for the K–12 organization and implement a maturation path in which progress is routinely evaluated to inform further investment. To ensure that their cybersecurity plan remains fit for this purpose, K–12 entities should participate in the free *Nationwide Cybersecurity Review (NCSR)*[22], which provides metrics that identify gaps and track progress, as well as access to incident reporting and cybersecurity resources. CISA and MS-ISAC use NCSR anonymized data to better prioritize programs and efforts that support SLTT government partners, including the K–12 community.[23]

RECOMMENDATION 2:

RECOGNIZE AND ACTIVELY ADDRESS **RESOURCE CONSTRAINTS**

Most school districts are doing a lot with a little. There is a clear need for increased cybersecurity budgeting and support mechanisms across the community. This resource shortfall is a major constraint to implementing effective cybersecurity programs across all K–12 entities.

To this end, CISA recommends that K–12 organizations take four key steps:

FIRST, *work with state planning committees* to leverage the *State and Local Cybersecurity Grant Program (SLCGP)* managed by CISA and the Federal Emergency Management Agency (FEMA). SLCGP will provide grants totaling one billion dollars to U.S. state, local, territorial, and tribal (SLTT) governments over the next four years. The 50 states, five territories, and District of Columbia are eligible to apply via each state/territory/district administrative agency. Participation in the SLCGP requires each state, territory, or district to establish a cybersecurity planning committee that coordinates, develops, and approves a cybersecurity plan, which must include at least one representative from "institutions of public education … within the jurisdiction of the eligible entity".[24] Leveraging these cybersecurity planning committees can result in improved strategic and resource cyber planning, cyber grant funding proposals, consolidated technical service requests, and information sharing across the K–12 community. K–12 organizations should also consider leveraging the *Homeland Security Grant Program (HSGP)*[25], which dedicates 7.5 percent of funds to support critical infrastructure cybersecurity.

Moreover, as noted in the October 2022 GAO report, the Federal Communications Commission (FCC) provides support to K-12 entities through the schools and libraries universal service support program, commonly known as the E-Rate program.[26] This program subsidizes telecom and broadband-related services to and within schools, primarily focusing on basic connectivity but including certain cybersecurity services like basic firewall protection services. In the wake of the recent ransomware attack on the Los Angeles Unified School District,[27] a group of stakeholders requested that the FCC expand its cybersecurity support.[28] In response to this and other requests, on December 14, 2022, the FCC requested public comment on whether it should permit the use of E-Rate funds to support advanced or next-generation firewalls and services, as well as other cybersecurity services.[29]

SECOND, *utilize free or low-cost services* to make near-term improvements in resource-constrained environments. For example, CISA has published a *Free Cybersecurity Services and Tools*[30] catalog, which provides a one-stop resource for K–12 entities of all sizes to find free public and private sector resources to reduce their cybersecurity risk. This page is frequently updated and an essential starting point for all organizations. Resources on this page are divided into several categories, including **(1)** reducing the likelihood of a damaging cyber incident; **(2)** detecting malicious activity quickly; **(3)** responding effectively to confirmed incidents; and **(4)** maximizing resilience.

THIRD, *ask more of technology providers*. Nearly all K–12 organizations rely on major technology companies for most of their IT functions. K–12 organizations should expect the technology used for core educational functions, like learning management and student administrative systems, to have strong security controls enabled by default for no additional charge. A key example is phishing-resistant MFA: K–12 organizations should demand that all core educational technology products have this critical security control enabled for all administrator accounts at minimum, at no additional cost to the K–12 organization. CISA will work with interested K–12 organizations on a set of expected security controls and secure-by-design attributes critical for all technologies used for high-priority functions.

FOURTH, *minimize the burden of security.* Identity services and mail systems are high-priority targets for attackers. As you consider ways to eliminate on-premises systems, prioritize those. Many K–12 organizations operate their own IT systems, known as "on premises." Such systems require time to patch, to monitor, and to respond to potential security events. Few K–12 organizations have the resources and expertise to keep them secure. CISA has observed that most smaller organizations across sectors cannot continuously handle the security and time commitments of running on-premises mail and file storage services, for example. K–12 organizations should urgently consider migrating on-premises IT services to the cloud. While it is not possible to categorically state that "the cloud is more secure," migration to the cloud will be a more secure and resilient option for many K–12 organizations.

RECOMMENDATION 3:

FOCUS ON COLLABORATION AND INFORMATION SHARING

K–12 entities struggle to fund cybersecurity resources while combating continuous threats. Situational awareness into changes in the risk environment is critical to ensure that resources are allocated to the most effective security mitigations and controls.

To achieve this, all K–12 organizations should participate in information-sharing forums such as MS-ISAC and K12 SIX, and consider working with other information-sharing organizations, such as fusion centers, state school safety centers, and other state and regional agencies. MS-ISAC membership offers unique opportunities. Registration enables reporting as well as data and information sharing. In addition, MS-ISAC K–12 community members receive critical alerts on current threats, risks, and vulnerabilities; free cyber tools, resources, and services; and 24/7 access to assistance that includes threat incident analysis, mitigation, and remediation.

K–12 organizations also should establish a relationship with their regional CISA cybersecurity advisor and local FBI field office. This will open lines of communication on evolving threats and risks and ensure prompt provision of U.S. government assistance to prevent and, where needed, respond to cybersecurity risks.[31] It is critical that K–12 organizations report every cyber intrusion to the U.S. government, every time. Reporting incidents allows CISA and our partners to offer incident response assistance, identify information that can be shared to help protect other potential victims, and better understand our adversary to develop more effective guidance and help law enforcement partners identify perpetrators. Any organization can report a cyber incident through the *Report to CISA* webpage,[32] and the FBI encourages internet crime victims to report to the Internet Crime Complaint Center.[33]

CONCLUSION

The education sector is foundational to U.S. strength and prosperity, but it is under unprecedented risk. Now more than ever, cyber actors are targeting our nation's education system and increased cybersecurity demands add strain to school districts that are already doing so much.

K–12 stakeholders and education sector partners informed and shaped this report, and we are grateful for the thoughts and expertise shared by those "on the ground." We learned that what the sector needs most is resources, **simplicity**, and **prioritization**. Accordingly, this report strives to cut through the noise and offer clear steps that are prioritized to help K–12 organizations implement the most effective cybersecurity controls first. Going forward, we will continue to work with the K–12 community, as well as other SLTT organizations, federal partners, and the private sector, to further improve CISA's support to the education sector.

ACKNOWLEDGEMENTS

CISA is deeply appreciative of contributions by many partners in development of this report, including the following organizations:

Council of Great City Schools

Consortium for School Networking

U.S. Department of Education

Federal Bureau of Investigation

Federal Communications Commission

Information Technology Sector Coordinating Council

(ISC)²

K12 Security Information eXchange (K12 SIX)

Michigan Department of Technology Management and Budget

Multi-State Information Sharing and Analysis Center

National Association of State Chief Information Officers

National Association of Elementary School Principals

National Association of Secondary School Principals

Palo Alto Unified School District

State Educational Technology Directors Association

Texas School Safety Center

APPENDIX 1:

K–12 RESOURCE REPOSITORY

FEDERALLY SUPPORTED RESOURCES ORGANIZED IN SUPPORT OF EACH REPORT RECOMMENDATION.

APPENDIX 1:
K–12 RESOURCE REPOSITORY

RECOMMENDATION 1 || Invest in the Most Impactful Security Measures and Build Toward a Cybersecurity Plan

Multifactor Authentication, CISA

Phishing-Resistant MFA Fact Sheet, CISA

Cyber Hygiene Services, CISA

Known Exploited Vulnerabilities Catalog, CISA

Get Your Stuff Off Search, CISA

Cross-Sector Cybersecurity Performance Goals, CISA

CPGs Checklist, CISA

Nationwide Cybersecurity Review (NCSR), CISA

Cybersecurity Framework, NIST

Cybersecurity Considerations for K–12 Schools and School Districts, Readiness and Emergency Management for Schools (REMS-TA)

Ransomware Guide (September 2020), CISA

K12 SIX Essential Cyber Incident Response Runbook (June 22, 2022), K12 SIX

State Cybersecurity Best Practices Incident Response Plan (Fall 2022), State Educational Technology Directors Association

RECOMMENDATION 2 || Recognize and Actively Address Resource Constraints

Free Cybersecurity Services and Tools, CISA

FY22 State and Local Cybersecurity Grant Program Fact Sheet, CISA

State and Local Cybersecurity Grant Program Frequently Asked Questions, CISA

Homeland Security Grant Program, FEMA

Homeland Security Grant Program (HSGP) Application Process, FEMA

RECOMMENDATION 3 || Focus on Collaboration and Information Sharing

Join MS-ISAC—Free for U.S. State, Local, Tribal & Territorial Government Entities, Center for Internet Security (CIS)

Report to CISA, CISA

Internet Crime Complaint Center (IC3), FBI

TRAINING FOR K–12 STUDENTS AND EDUCATORS:

Federal Virtual Training Environment (FedVTE) Public Courses

Foundations of Cybersecurity for Managers, National Initiative for Cybersecurity Careers and Studies (NICCS)

Fundamentals of Cyber Risk Management, NICCS

Don't Wake Up to a Ransomware Attack, NICCS

SchoolSafety.gov Cybersecurity Topic Page

Cybersecurity Training and Exercises, CISA

NICCS Education and Training Catalog

CETAP Cyber Safety Videos, Cyber.org and CISA Counselors

Cybersecurity Considerations for K–12 Schools and School Districts, REMS-TA Center

The Largest Cybersecurity Hacking Competition

APPENDIX 2:

KEY SOURCES

APPENDIX 2:
KEY SOURCES

Cyber Actors Target K–12 Distance Learning Education to Cause Disruptions and Steal Data

Joint Cybersecurity Advisory from CISA, FBI, and MS-ISAC (December 2020)

The FBI, CISA, and MS-ISAC assess malicious cyber actors are targeting kindergarten through 12th grade (K–12) educational institutions, leading to ransomware attacks, the theft of data, and the disruption of distance learning services. Cyber actors likely view schools as targets of opportunity, and these types of attacks are expected to continue through the 2020/2021 academic year. These issues will be particularly challenging for K–12 schools that face resource limitations; therefore, educational leadership, information technology personnel, and security personnel will need to balance this risk when determining their cybersecurity investments.

In these attacks, malicious cyber actors target school computer systems, slowing access, and—in some instances—rendering the systems inaccessible for basic functions, including distance learning. Adopting tactics previously leveraged against business and industry, ransomware actors have also stolen—and threatened to leak—confidential student data to the public unless institutions pay a ransom.

Cyber Threats to K–12 Remote Learning Education

(December 2020)

The Cybersecurity and Infrastructure Security Agency (CISA) has seen an increase in malicious activity with ransomware attacks against K–12 educational institutions. Malicious cyber actors are targeting school computer systems, slowing access, and rendering the systems inaccessible to basic functions, including remote learning. In some instances, ransomware actors stole and threatened to leak confidential student data unless institutions paid a ransom.

Additionally, this report covers common cyber terms and concerns along with general cybersecurity best practices, video conferencing best practices, and information resources.

Cybersecurity Recommendations for K–12 Schools Using Video Conferencing Tools and Online Platforms – Fact Sheet

(May 13, 2020)

K–12 school districts are increasingly incorporating distance learning tools as a means of delivering curricula. Advances in information technology as the increased availability of video conferencing software and video conferencing capabilities incorporated into other products have rapidly made distance learning more feasible. However, schools and school districts must balance the convenience, usability, speed, and stability of these platforms with increasing risks to both school IT networks and individual users.

Additionally, this report covers additional threat vectors, to include nation-state, insiders, and criminal organizations. Further, this product provides recommended security practices for K–12 organizations.

APPENDIX 2:
KEY SOURCES

Stop Ransomware: K–12 Resources—**CISA Webpage** (January 2021)

This webpage was created in January 2021, in response to the rise in malicious activity with ransomware attacks against K–12 educational institutions since the onset of COVID-19 and the increase in remote learning. Additionally, this webpage provides information for the "reduce the risk of ransomware campaign," "ransomware reference materials to K–12 school and school district IT staff," "ransomware reference materials for parents, teachers, and school administrators," and "ransomware reference materials for students."

MS-ISAC and CISA—**Ransomware Guide** (September 2020)

On September 30, 2020, a joint Ransomware Guide was released, which is a customer centered, one-stop resource with best practices and ways to prevent, protect and/or respond to a ransomware attack. CISA and MS-ISAC are distributing this guide to inform and enhance network defense and reduce exposure to a ransomware attack:

This Ransomware Guide includes two resources:

- *Part 1: Ransomware Prevention Best Practices*
- *Part 2: Ransomware Response Checklist*

K–12 Education Leaders' Guide to Ransomware: Prevention, Response, and Recovery Webinar (1 hour) (March 2021)

The K–12 Education Leaders' Guide to Ransomware: Prevention, Response, and Recovery Webinar, hosted by CISA and the National Cyber Security Alliance (NCSA), focuses on the steps K–12 schools can take to prevent (before), respond to (during), and recover from (after) ransomware attacks, as well as free services that administrators can utilize to protect their schools.

#StopRansomware: Vice Society (Sept. 7, 2022) Joint Cybersecurity Advisory from CISA, FBI, and MS-ISAC

Over the past several years, the education sector, especially kindergarten through twelfth grade (K–12) institutions, have been a frequent target of ransomware attacks. Impacts from these attacks have ranged from restricted access to networks and data, delayed exams, canceled school days, and unauthorized access to and theft of personal information regarding students and staff. The FBI, CISA, and the MS-ISAC anticipate attacks may increase as the 2022/2023 school year begins and criminal ransomware groups perceive opportunities for successful attacks. School districts with limited cybersecurity capabilities and constrained resources are often the most vulnerable; however, the opportunistic targeting often seen with cyber criminals can still put school districts with robust cybersecurity programs at risk. K–12 institutions may be seen as particularly lucrative targets due to the amount of sensitive student data accessible through school systems or their managed service providers.

FOOTNOTES

[1] Alert (AA22-249A) #StopRansomware: Vice Society," Cybersecurity and Infrastructure Security Agency, last modified September 8, 2022, https://www.cisa.gov/uscert/ncas/alerts/aa22-249a.

[2] The information in this report is being provided "as is" for INFORMATIONAL PURPOSES ONLY. CISA does not endorse any commercial product or service, including any subjects of analysis. Any reference to specific commercial entities or commercial products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply endorsement, recommendation, or favoritism by CISA.

[3] Levin, Douglas A. (2022). "The State of K–12 Cybersecurity: Year in Review, 2022 Annual Report," K12 Security Information Exchange, accessed December 5, 2022, https://www.k12six.org/the-report.

[4] "Data Security: Recent K–12 Data Breaches Show That Students Are Vulnerable to Harm," GAO, GAO-20-644 (Washington, D.C.: Sept. 15, 2020), accessed December 5, 2022, https://www.gao.gov/products/gao-20-644.

[5] "The Tsunami Threat of K–12 Cybersecurity," The Consortium for School Networking (CoSN), accessed December 5, 2022, https://www.cosn.org/the-tsunami-threat-of-K–12-cybersecurity/.

[6] "New MS-ISAC Report Details Cybersecurity Challenges of K–12 Schools," Center for Internet Security, accessed December 5, 2022, https://www.cisecurity.org/about-us/media/press-release/new-ms-isac-report-details-cybersecurity-challenges-of-K–12-schools.

[7] "Critical Infrastructure Protection: Additional Federal Coordination Is Needed to Enhance K–12 Cybersecurity," GAO, GAO-23-105480 (Washington, D.C.: October 2022), accessed December 5, 2022, https://www.gao.gov/assets/gao-23-105480.pdf

[8] Ibid.

[9] Levin, Douglas A. (2022). "The State of K–12 Cybersecurity: Year in Review, 2022 Annual Report," K12 Security Information Exchange, accessed December 5, 2022, https://www.k12six.org/the-report.

[10] "Finalsite ransomware attack forces 5,000 school websites offline," TechCrunch, accessed December 5, 2022, https://techcrunch.com/2022/01/07/finalsite-ransomware-school-websites-offline/.

[11] "2022 CoSN EdTech Leadership Survey Report," CoSN, accessed on December 13, 2022, https://www.cosn.org/edtech-topics/state-of-edtech-leadership/.

[12] "Multifactor Authentication," Cybersecurity and Infrastructure Security Agency, accessed December 5, 2022, https://www.cisa.gov/mfa.

[13] For a description of implementing phishing-resistant MFA, see https://www.cisa.gov/sites/default/files/publications/fact-sheet-implementing-phishing-resistant-mfa-508c.pdf.

[14] "Cyber Hygiene Services," Cybersecurity and Infrastructure Security Agency, accessed December 5, 2022, https://www.cisa.gov/cyber-hygiene-services.

[15] "Known Exploited Vulnerabilities Catalog," Cybersecurity and Infrastructure Security Agency, accessed December 5, 2022, https://www.cisa.gov/known-exploited-vulnerabilities-catalog.

[16] "Get Your Stuff Off Search," Cybersecurity and Infrastructure Security Agency, accessed December 5, 2022, https://www.cisa.gov/publication/stuff-off-search.

FOOTNOTES

[17] Private sector entities, including Amazon, CYBER.ORG, and the SANS Institute, also offer free training. Each K–12 organization should assess its training needs and take full advantage of the breadth of available free resources.

[18] "Cross-Sector Cybersecurity Performance Goals," Cybersecurity and Infrastructure Security Agency, accessed December 5, 2022, https://www.cisa.gov/cpg.

[19] Cybersecurity and Infrastructure Security Agency, CPGs Checklist, October 26, 2022, https://www.cisa.gov/sites/default/files/publications/CISA_CPG_CHECKLIST_508c.pdf.

[20] "Cross-Sector Cybersecurity Performance Goals," Cybersecurity and Infrastructure Security Agency, accessed November 30, 2022, https://www.cisa.gov/cpg.

[21] "Cybersecurity Framework," National Institute for Standards and Technology, accessed December 5, 2022, https://www.nist.gov/cyberframework.

[22] "Nationwide Cybersecurity Review (NCSR)," Center for Internet Security, accessed November 30, 2022, https://www.cisecurity.org/ms-isac/services/ncsr.

[23] Ibid.

[24] "State and Local Cybersecurity Grant Program Frequently Asked Questions," Cybersecurity and Infrastructure Security Agency, accessed November 30, 2022, https://www.cisa.gov/cybergrants-faq.

[25] "Homeland Security Grant Program," Federal Emergency Management Agency, accessed November 30, 2022, https://www.fema.gov/grants/preparedness/homeland-security.

[26] "Critical Infrastructure Protection: Additional Federal Coordination Is Needed to Enhance K–12 Cybersecurity," GAO, GAO-23-105480 at 7 (Washington, D.C.: October 2022).

[27] Associated Press, "A Cyberattack Hits the Los Angeles School District, Raising Alarm Across the Country," (Sept. 7, 2022), accessed December 9, 2022, https://www.npr.org/2022/09/07/1121422336/a-cyberattack-hits-the-los-angeles-school-district-raising-alarm-across-the-coun.

[28] Letter from Local Educational Agencies and Organizations to FCC Chairwoman Jessica Rosenworcel et al., (Sept. 21, 2022), accessed December 9, 2022, https://www.fcc.gov/ecfs/document/10922246829893/1.

[29] *Wireline Competition Bureau Seeks Comment on Requests to Allow the Use of E-Rate Funds for Advanced or Next-Generation Firewalls and other Network Security Services*, WC Docket No. 13-184, Public Notice, DA 22-1315, at Appendix A (rel. WCB Dec. 14, 2022), https://www.fcc.gov/document/wcb-seeks-comment-e-rate-eligibility-advanced-firewalls.

[30] Free Cybersecurity Services and Tools," Cybersecurity and Infrastructure Security Agency, accessed November 30, 2022, https://www.cisa.gov/free-cybersecurity-services-and-tools.

[31] For information about CISA's regional cybersecurity personnel, see www.cisa.gov/cisa-regions.

[32] "Report to CISA," Cybersecurity and Infrastructure Security Agency, accessed December 5, 2022, https://www.cisa.gov/report.

[33] To file a complaint with the Internet Crime Complaint Center, see https://www.ic3.gov/.