K-12 DIGITAL INFRASTRUCTURE BRIEF:

DEFENSIBLE & RESILIENT

August 2023

Version 1.0

Examples Are Not Endorsements

This document contains examples and resource materials that are provided for the user's convenience. The inclusion of non-Federal resources in this document is not intended to reflect its importance, nor is it intended to endorse any views expressed, initiatives, or products or services offered. Any opinions expressed in these materials do not necessarily reflect the positions or policies of the U.S. Department of Education or the Federal government. The U.S. Department of Education does not control or guarantee the accuracy, relevance, timeliness, or completeness of any outside information included in these materials.

Licensing and Availability

This report is available on the Department's Website at http://tech.ed.gov.
Requests for alternate format documents such as Braille or large print should be submitted to the Alternate Format Center by calling **1-202-260-0852** or by contacting the 504 coordinator via email at **om_eeos@ed.gov**.

Notice to Limited English Proficient Persons

If you have difficulty understanding English, you may request language assistance services for Department information that is available to the public. These language assistance services are available free of charge. If you need more information about interpretation or translation services, please call **1-800-USA-LEARN (1- 800-872-5327) (TTY: 1-800-437-0833)** or email us at: **Ed.Language.Assistance@ed.gov**. Or write to: U.S. Department of Education, Information Resource Center, LBJ Education Building, 400 Maryland Ave. SW, Washington, DC 20202.

Contents

Acknowledgments

Project Team

The 2023 K–12 Digital Infrastructure Brief was published by the U.S. Department of Education, Office of Educational Technology (OET).

Michael Klein served as the principal lead in developing the brief with support from **Zac Chase**. Within OET **Bernadette Adams, Jessica Ch'ng, Yenda Prado, Ellery Robinson,** and **Ji Soo Song** provided technical assistance, under the guidance of **Kristina Ishmael** and **Roberto Rodriguez.**

Additional 2023 K–12 Digital Infrastructure Brief support was provided by the following K–12 Chief Technology Officers and other subject matter experts: **Douglas Alexander** (OSHEAN), **Valarie Byrd** (South Carolina Department of Education), **Doug Casey** (CCET, Connecticut Commission on Educational Technology), **Jennifer Covington** (Murray City School District), **Christine Fox** (CAST), **Ryan Kocsondy** (CEN, Connecticut Education Network), **Kim Lewis** (CENIC), **Amy Lewis Land** (Town of New Shoreham), **Mary McCarvel-O'Connor** (North Dakota Department of Public Instruction), **Pam McLeod** (Concord School District), **Joshua Olstad** (Oyster River Cooperative School District), **Kristi Peak-Oliveira** (Easterseals Massachusetts), **Sean Osborne** (South Carolina Department of Education), **Steve Smith** (A4L, Access 4 Learning), and **Darrell Williams** (Wisconsin Department of Public Instruction).

The following individuals provided additional assistance and support of the 2023 K-12 Digital Infrastructure Brief: **Susan Bearden** (InnovateEDU), **Lindsay Burton** (CISA), **Alaina Clark** (CISA), **Julia Fallon** (SETDA, The State Education Technology Directors Association), **Arlene Guevara-Zuleta** (CISA), **Kevin Herms** (U.S. Department of Education), **Angela Hernandez** (U.S. Department of Education), **Keith Krueger** (CoSN, The Consortium for School Networking), **Doug Levin** (K12 SIX, the K12 Security Information eXchange), **Amy McLaughlin** (CoSN), **Seeyew Mo** (ONCD, Office of the National Cyber Director), **Erin Mote** (InnovateEDU), **Ruth Ryder** (U.S. Department of Education), **Ryan Streeter** (CISA), **Valerie Truesdale** (AASA, the School Superintendents Association), **Mark Washington** (U.S. Department of Education), and **Bryan Williams** (U.S. Department of Education).

Introduction & Overview

This is the second in a series of five briefs[1] published by the U.S. Department of Education Office of Educational Technology on the key considerations facing educational leaders as they work to build and sustain core digital infrastructure for learning. These briefs offer recommendations to complement the fundamental infrastructure considerations outlined in the 2017 update to Building Technology Infrastructure for Learning. They are meant to provoke conversations, challenge conventions, and deepen understanding. These briefs have been purposefully designed to be easily consumed and shared.

The needs, capabilities, and expectations of technology infrastructure vary significantly by context. A rural outdoor learning school in the mountainous American Southwest will face challenges and have needs much different than a district within an urban center along the East Coast with an all-digital curriculum. The recommendations within these briefs are meant to help build, augment, and sustain digital infrastructure supportive of learning no matter the location.

America has made incredible progress in closing the digital access divide,[2] providing an ever-greater proportion of students with access to broadband connectivity, devices, and digital resources. At the same time, we must acknowledge the last frontiers of connectivity can also present the most wicked problems[3] of closing that divide. To help readers build solutions for their own contexts, these briefs offer examples from the field of those who faced pernicious challenges to connectivity, accessibility, cybersecurity, data privacy, and other infrastructure issues and designed solutions for their challenges. More examples can also be found at tech.ed.gov/stories.

Education Infrastructure is Critical Infrastructure

Education's digital infrastructure is officially considered critical infrastructure,[4] and just as we work to provide physical infrastructure that is safe, healthy, and supportive for all students, we need to align resources to create digital infrastructure that is safe, accessible, resilient, sustainable, and future-proof. Digital infrastructure includes "the resources that make digital systems possible and how individuals and organizations access and use these resources."[5] This considers the complex interplay of people, processes, and tools, including elements such as connectivity, security, interoperability, accessibility, affordability, and digital literacy as well as "behavioral, social, and physical barriers and opportunities for equitable adoption who uses and does not use digital technologies and why."[6]

[1] The inclusion of non Federal resources in this document is not intended to reflect its importance, nor is it intended to endorse any views expressed, initiatives, or products or services offered. Any opinions expressed in these materials do not necessarily reflect the positions or policies of the U.S. Department of Education or the Federal government. The U.S. Department of Education does not control or guarantee the accuracy, relevance, timeliness, or completeness of any outside information included in these materials.

[2] https://www.gao.gov/blog/closing-digital-divide-millions-americans-without-broadband

[3] https://www.stonybrook.edu/commcms/wicked-problem/about/What-is-a-wicked-problem

[4] The Education Facilities Subsector (EFS) within Government Facilities Sector was established with ED identified as the corresponding Sector Specific Agency (SSA) in the 2006 National Infrastructure Protection Plan (NIPP). The designation of EFS as "critical infrastructure" and ED s role as the agency responsible for the EFS has been reaffirmed in the 2009 NIPP, 2013 NIPP, Presidential Policy Directive 21, and, most recently, in Section 9002 of the Fiscal Year 2021 National Defense Authorization Act (NDAA). The 2021 NDAA renamed SSAs as Sector Risk Management Agencies (SRMAs) and articulated specific SRMA responsibilities. https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/national-infrastructure-protection-plan-and-resources

[5] Borrowing from the USAID' definition in their August 2022 Digital Ecosystem Framework: https://www.usaid.gov/sites/default/files/2022-05/Digital_Strategy_Digital_Ecosystem_Final.pdf

[6] https://www.usaid.gov/sites/default/files/2022-05/Digital_Strategy_Digital_Ecosystem_Final.pdf

What Are We Working Toward?

To understand this imperative, consider the following hypothetical scenario, outlining one of many possibilities when digital infrastructure is operating optimally.

A Guiding Scenario[7]

A middle school principal opens a pre-meeting of school personnel who are part of the multidisciplinary team for an upcoming Individualized Education Program (IEP) meeting to discuss any anticipated revisions and opportunities for additional services. The case manager starts by pulling up a school-wide dashboard showing trends in the school's academic, attendance, and wellness data and showing how the student's data aligns with schoolwide data.

As the team navigates the student profile—a dashboard with the student's picture, grades, attendance, interests, and IEP goals—a special educator points out that the student has made progress on math goals but has continued to struggle with reading comprehension.

The Speech Language Pathologist (SLP) proposes that the student be considered for assistive technology (AT) services, which would include an evaluation of the student to determine whether and what AT could aid in addressing current learning needs. The proposal would include the ability for staff to safely collect the data they need to monitor the intervention's effectiveness and securely share the data with other systems like the student profile the team is currently reviewing. The Assistant Principal (AP) notes that in order to ensure that the AT evaluation also addresses the district's cybersecurity and data privacy requirements, the process would need to include input from the district's IT personnel. The AP asks the SLP to proceed with exploring this option, coordinate with IT staff, and copy the AP on emails to ensure that the various departments—special education, procurement, and IT continue to coordinate.

One of the student's general education teachers at the meeting notes the student's family is part of the district's affordable connectivity partnership with local internet providers and volunteers to include as part of the AT service proposal, a series of virtual meetings with the student and their family to demonstrate how to use the technology at home. The teacher, seeing a note on the dashboard that one of the student's parents is deaf, writes a reminder to re-familiarize himself with the contracted interpreter services and closed captioning function of the district's virtual conferencing platform. By taking these steps, the team ensures that the technology that best meets the student's needs also works with existing district tools and keeps the network secure prior to inclusion within the student's IEP.

The scenario above demonstrates the safe, effective, and helpful use of technology in support of learning and highlights the interplay of tools and processes, as well as the individual and organizational capacity that enables the use of technology to support students. Such scenarios rely on the following key tenets of digital infrastructure, which also guide the organization of this resource:

[7] It is important to note that personally identifiable data, information, and the education records of a student with a disability must be protected consistent with the Family Educational Rights and Privacy Act (FERPA) and the confidentiality protections of the Individuals with Disabilities Education Act (IDEA).

Key Tenets of Digital Infrastructure

1

Digital infrastructure should be adequate and future-proof. Connections, speeds, and devices should be designed to meet the needs of modern education with plans for financial sustainability. This infrastructure should also be scalable to meet future needs.

2

Digital infrastructure should be defensible and resilient. Cybersecurity risk presents both a management and technical challenge. Ensuring the safety of people, data, and systems requires continuously building capacity to mitigate and respond to current risks like ransomware, as well as evolving cyber threats.

3

Digital infrastructure should be privacy-enhancing, interoperable, and useful. By prioritizing privacy and ensuring data protection measures, schools build trust with stakeholders and maintain the confidentiality and integrity of sensitive student data. Embracing interoperability standards can enable the seamless exchange of data between systems, empowering educators to make informed decisions and personalize learning experiences. Adherence to interoperability and privacy standards should be required from any third-party vendor or developer considered for inclusion within that infrastructure. Furthermore, personal data connected with users should be portable, allowing authorized users to take it with them and share it within and between educational systems.

4

Digital infrastructure should be accessible to individuals with disabilities and multilingual learners. Schools must provide equal access to individuals with disabilities. Planning for accessibility at all stages of the technology lifecycle—procurement, implementation, training, and support—as well as ensuring alignment to key accessibility-related frameworks and guidelines helps ensure that a school's digital infrastructure is readily accessible to individuals with disabilities. Schools must also take reasonable steps to ensure meaningful access to their programs and activities to people with limited English proficiency, which may include the use of multilingual digital content.

5

Digital infrastructure should enhance student digital health, safety, and citizenship skills. Digital infrastructure should be designed to protect and improve the digital health, safety, and citizenship[8] skills of the people within that system, including the privacy of their data. The existence and expansion of all such infrastructure should include clear plans for how to educate the end users and custodians of those systems in building and maintaining digital health, safety, and citizenship skills.

[8] Digital citizenship is appropriate, responsible behavior when using technology, including social media, websites, online forums, communities, comments, and apps and other device features. Teaching children and teens digital citizenship skills can help prevent cyberbullying and its negative effects. When children learn positive online behaviors, social media can be used in productive ways. (source: Digital Citizenship Skills | StopBullying.gov)

Whose Job is It?

Building and maintaining safe, accessible, resilient, and effective digital infrastructure is a whole-of-community challenge requiring whole-of-community solutions. While every person has a role to play, the following groups play key roles:

- **District Leaders:** As organizational leaders, superintendents and senior district leaders play an important role in prioritizing secure digital infrastructure across the district and owning cyber risk management and digital accessibility at the executive leadership level. Put differently, if someone needs to announce a closure due to a cyberattack or answer questions from the board or press, it is likely to be the superintendent. To proactively address those risks, district leaders can focus the time, attention, and resources of students, staff, and leadership on practices that support secure, privacy-enhancing, accessible, and interoperable digital infrastructure
- **District Technology Leaders:** As the primary implementers and maintainers of a district's digital infrastructure, chief technology officers and IT directors are often responsible for carrying out key aspects of mitigating cyber risk and supporting powerful teaching and learning for all students and staff. Technology leaders can create a culture of trust and security awareness by building processes for collaboration and coordination with students, staff, leadership, and outside experts. Technology leaders can also create the conditions for accessibility for all users by working closely with vendors during the design and procurement stages, and, when feasible, including individuals with disabilities in those processes
- **Educators:** As the group tasked with facilitating high-quality teaching and learning to all students, educators (including general educators, special educators, related service providers, paraprofessionals, and others) often see the greatest possibilities and most frustrating constraints when it comes to digital infrastructure. As those often closest to the educational and social-emotional needs of students, educators seek out the most effective tools to meet their students' needs. They can have a powerful impact by practicing essential cyber hygiene and modeling it for students and families. By collaborating with IT/technology professionals to consider cybersecurity, data privacy, and accessibility when reviewing digital tools, educators can help to ensure all students have access to safe, secure, accessible, and powerful learning experiences.
- **Students and Families:** In partnership with schools and communities, families can collaborate with teachers and support secure access to digital infrastructure at home. Feedback from students and families can be an important way for schools to understand when tools or experiences are inaccessible, when data in progress reports are confusing, or when they feel unsafe in school or online. Students and families can also advocate that districts and vendors protect the privacy of students' data. For more on student data privacy and federal laws see K–12 Digital Infrastructure Brief: Privacy-enhancing, Interoperable, and Useful.
- **State Leaders:** State educational agency (SEA) leaders help support educational technology (edtech) infrastructure by modeling institutional best practices, developing thoughtful policy and guidance, and providing adequate resourcing to support policy implementation. For example, SEA staff may leverage the Office of EdTech's 2023 Dear Colleague Letter to help districts plan for and use their federal education funds to support digital equity, including hiring instructional coaches and providing professional learning for educators.

- **Vendors and Service Providers:** Vendors and service providers play an outsized role in the privacy, security, accessibility, and interoperability of K–12 digital infrastructure. The K–12 education sector's reliance on third-party providers includes costs and benefits. While each vendor and service provider adds supply chain risks that can be opaque and challenging to mitigate, these providers often provide services districts cannot support and maintain on their own, such as secure backups and cloud storage, as well as web templates, electronic portals, and applications. In addition, some vendors invest substantial resources in cybersecurity and data privacy (often more than a district could afford on its own). Finally, improvements in the security posture or digital accessibility of a vendor or service provider used widely in K–12 can benefit thousands of school districts, rather than needing to fix vulnerabilities or accessibility barriers district by district.

And many more: Within school districts, district and school staff interact regularly with sensitive student and staff data, while district leaders in special education, finance, human resources, operations, and curriculum play important roles in managing risk and ensuring accessibility. Educational service agencies (ESAs) often help build the capacity of thousands of school districts across the country, sometimes by managing a district's entire digital infrastructure. Federal partners like the U.S. Department of Education (ED),[9] Cybersecurity and Infrastructure Security Agency (CISA), Federal Bureau of Investigation (FBI), and others play a critical role in providing technical assistance, sharing intelligence and analysis, and investigating criminal cyber activity, while the Federal Communications Commission provides vital funding via the eRate program.

[9] ED has limited authorities related to K–12 cybersecurity. The 2013 National Infrastructure Protection Plan (NIPP) and the FY21 National Defense Authorization Act (NDAA) designated ED as the Education Facilities Subsector (EFS) Sector Risk Management Agency (SRMA). Within current authorities, ED can provide technical assistance related to K–12 cybersecurity.

Key Considerations

Key considerations within this brief include:

Continuous Risk Management: Cybersecurity should be approached as a continuous process of managing risk. It is important to recognize the inherent insecurity in digital infrastructure and implement processes to reduce the risk of exposure.

Analogies for Understanding: Drawing analogies from the physical world, such as school fire safety, can help educators, leaders, and community members understand and address cybersecurity challenges.

Prioritization and Mitigation: It is important to prioritize the greatest risks and implement mitigations accordingly. CISA and ED recommend implementing multi-factor authentication (MFA), enforcing minimum password strength, recognizing and reporting phishing attempts, and keeping software updated (by patching known exploited vulnerabilities) as the highest-impact mitigations districts can take to reduce cybersecurity risk.

Prepare for When, not If: Prepare for responding to and recovering from a cybersecurity incident to bolster the resilience of your organization. We recommend developing and exercising a cyber incident response plan, running a ransomware tabletop exercise for the executive leadership team, and practicing restoring your critical systems from backups.

Vendors Have a Key Role to Play: Vendors should prioritize cybersecurity measures and investments to enhance the defensibility and resilience of their customers' systems. In addition to the mitigations recommended to districts, vendors should design their systems to be secure by design, obtain certifications from recognized authorities to provide cyber risk assurance, and implement security vulnerability disclosure practices.

Digital Infrastructure Should be Defensible and Resilient

Finding the Right Analogy: Fire Safety and Cybersecurity

Finding analogies in the physical world can help us frame and solve challenges in the digital world. Experience with school fire safety in the world of physical infrastructure has been a helpful analogy for approaching cybersecurity in the world of digital infrastructure.

Tools: When a district designs, builds, and maintains a school, they intend to prevent fires from occurring by using fire-resistant materials and safe wiring practices. However, based on real world experience and risk assessment, they assume that fires may occur. So, leaders need to build systems that will allow people, processes, and tools to detect, respond to, and recover from fires in ways that mitigate harm to people and damage to the learning environment. Smoke detectors, alarms, and sprinklers in each classroom ensure automated detecting, alerting, and response. Fire extinguishers and pullable fire alarms in the hallways allow humans to intervene when automated systems don't work (and provide a way to track who pulled the alarm in case of misuse). Specialized controls protect the riskiest contexts like science labs and kitchens. Ramps, visual alarms, and automatic doors ensure accessibility so all people can safely evacuate the building in case of a fire.

People and Process: Beyond the tools, there's an understanding that fire safety is a whole-of-community effort where each person has a role to play. Multiple times a year, schools engage in fire drills in collaboration with their local fire department. Teachers grab their emergency folders with maps, rosters, and emergency contact information. All staff members help students follow the proper procedures for safely evacuating the building while the principal assesses the effectiveness of the exercise with their local fire safety experts.

Similarly, as leaders, we should be able to envision what it looks like to design, build, and maintain defensible and resilient digital infrastructure and how we align the people, processes, and tools to do it.

A Threat-Informed, Risk-Based Approach to Cybersecurity

According to the National Cybersecurity Strategy, released by the White House in March 2023, digital infrastructure should be "**Defensible**, where cyber defense is overwhelmingly easier, cheaper, and more effective," and "**Resilient**, where cyber incidents and errors have little widespread or lasting impact."[11]

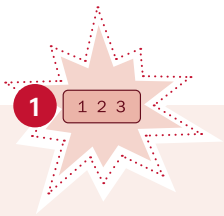
From 2016–2022, K–12 public schools and districts experienced at least 1,619 cybersecurity-related incidents including ransomware attacks, data breaches, phishing, and denial-of-service attacks.[12] Ransomware has had profound impacts on teaching, learning, and operations across the country—shutting down school districts after rendering their digital infrastructure inoperable, extorting ransom payments from school districts struggling to reopen, and exposing extremely sensitive student and staff personally identifiable information (PII) in highly publicized data breaches.

Add to that threat environment the challenges of the scale of the K–12 education system and its resource constraints. Roughly 70 percent of the 14,000 school districts in the United States have fewer than 2,500 students. Many of those districts have one or two IT staff members or have outsourced IT functions to an ESA or managed services provider. While edtech leaders have ranked cybersecurity as their number one concern from 2018–2023, only one-third of school districts have a full-time employee dedicated to cybersecurity.[13] Our policies and practices need to grapple with that reality.

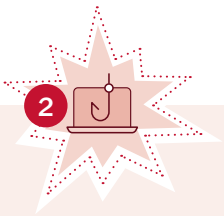
[11] https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/02/fact-sheet-biden-harris-administration-announces-national-cybersecurity-strategy/
[12] https://www.k12six.org/map
[13] https://www.cosn.org/wp-content/uploads/2023/05/Survey_Report_2023_F2.pdf

High-Impact Recommendations

Prioritization of the greatest risks and mitigations can begin to address these challenges. Many malicious cyber actors gain initial access in one of three ways:[14]



Compromising valid accounts, often with weak or stolen credentials



Phishing users with a malicious link or attachment

Exploiting unpatched known vulnerabilities in public-facing applications

In October 2022, ED, the U.S. Department of Homeland Security, the U.S. Department of Justice (DOJ), and the U.S. Department of Health and Human Services (HHS) jointly released a 1-page set of Cybersecurity Action Steps for the K–12 Community, which details steps that districts can take to dramatically reduce their cybersecurity risk and potential liability:

Enable Multi-Factor Authentication (MFA)

Use strong, unique passwords for every account

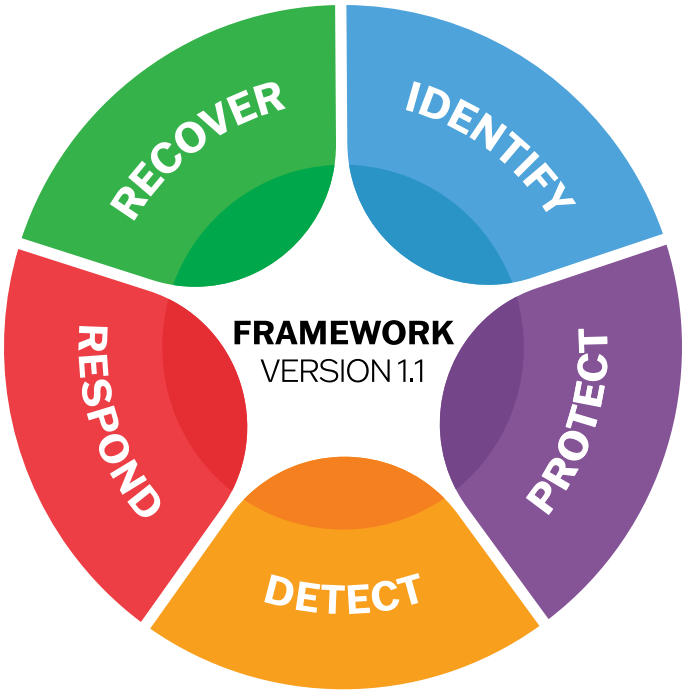
Recognize and report phishing

Update your software

Additionally, in January 2023 CISA released Protecting Our Future: Partnering to Safeguard K–12 Organizations from Cybersecurity Threats and a supporting Online Toolkit, which emphasized ways to minimize the burden of security. 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. As you consider ways to eliminate on-premises systems, prioritize identity services and mail systems, which are high-priority targets for attackers. 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.

[14] https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-137a

Framing Cybersecurity Risk Management:[15] Organizational leaders must think strategically about how to approach cyber risk. The core functions of the National Institute of Standards and Technology (NIST) Cyber Security Framework (CSF) Version 1.1—Identify, Protect, Detect, Respond, and Recover—organize cybersecurity activities at their highest level.[16] We structure the sections below around the five core functions in NIST 1.1 to help districts strategically approach cybersecurity risks and build a more defensible and resilient digital infrastructure.



CISA's Cross-Sector Cybersecurity Performance Goals (CPGs)

CISA's Cross-Sector Cybersecurity Performance Goals (CPGs), released in October 2022 and updated in March 2023, can help schools prioritize limited resources. The CPGs are a user-friendly set of cybersecurity best practices aligned to the NIST CSF that any school district or state agency technology leader can pick up and start using today. Several of the highest-impact goals are highlighted below.

[15] For K–12 leaders interested in learning more about purpose, structure, similarities, and differences of three of the most popular cybersecurity frameworks used by K–12 institutions, see Cybersecurity Frameworks: What K–12 Leaders Need to Know published by State Educational Technology Directors Association (SETDA) and K12 Security Information Exchange (K12 SIX) in October 2022. The Frameworks considered include NIST CSF 1.0, the Center for Internet Security's (CIS) Critical Security Controls, and the K–12 specific K12 SIX Essential Cybersecurity Protections.

[16] As of August 2023, NIST is in the process of developing NIST CSF 2.0 and anticipates a Winter 2024 release date. In addition to the five core functions identified in NIST CSF 1.1, NIST CSF 2.0 will add "Govern" as a sixth function https://www.nist.gov/system/files/documents/2023/01/19/CSF_2.0_Concept_Paper_01-18-23.pdf

Identify

According to NIST, "the Identify Function assists in developing an organizational understanding to managing cybersecurity risk to systems, people, assets, data, and capabilities."[17] With the average school district leveraging over 1400 edtech tools each month during the 2022–2023 school year,[18] assessing and prioritizing cybersecurity risks and mitigations is vital to ensuring the defensibility and resilience of a district's digital infrastructure. While all districts are unique, many districts have found the following practices helpful in identifying and mitigating cyber risk.

Identify the Crown Jewels and Conduct an Asset Inventory (CPG 1.A)

Since cyber risk management is a process of prioritizing risks, leaders should start by identifying the greatest cybersecurity threats to learning and operations. When identifying these most critical risks, answer these questions:

- Which systems are so critical to learning and operations that we would likely have to cancel school if they were rendered inoperable?
- Which systems contain data that is so sensitive or important that an attack on the confidentiality, integrity, or availability of the system would likely cause devastating physical, psychological, reputational, or legal harm to students, families, staff, or the institution?

Some of the most critical systems often include education sector-specific tools like a student information system (SIS), learning management system (LMS), IEP management system, enterprise resource planning (ERP) system (for payroll, HR, finance, etc.), food service system, and transportation system. These systems may also include general enterprise IT systems such as a virtual private network (VPN), identity and access management (IAM), cloud storage, physical and virtual servers, and productivity software, as well as heating, ventilation, and air conditioning (HVAC) and building access systems.[19]

Identify Organizational Cybersecurity Leadership (CPG 1.B)

Since cybersecurity is an essential risk management function for organizational leadership, successful organizations often have a role or position that is identified as responsible and accountable for the planning, resourcing, and execution of cybersecurity activities. While some large school districts may have a dedicated staff member like a Chief Information Security Officer, most districts will not have the resources for a dedicated role and may need to add specific cybersecurity roles to existing positions like IT Director or Chief Technology Officer. The Consortium for School Networking (CoSN) CEO Keith Kruger noted, "Cybersecurity is the top concern of district IT leaders. Yet, when we ask if districts have the human capacity to address cybersecurity, they clearly do not."[20] To address this problem, in October 2022 CoSN and The State Education Technology Directors Association (SETDA) published a Cybersecurity Staffing Resource for K–12 to provide concrete strategies to system leaders trying to address cybersecurity.

Mitigate Known Exploited Vulnerabilities (CPG 1.E)

Cybersecurity threats can feel overwhelming given limited resources in terms of time, staff, and funding. CISA and ED strongly encourage organizational cybersecurity leaders to focus on identifying and mitigating known exploited vulnerabilities: the small subset of vulnerabilities that are being actively exploited in the wild and have clear remediation actions to mitigate against that immediate harm. As a state or district cybersecurity leader, there are three immediate actions to address this challenge, all of which are free:

- **Sign up for CISA's Cyber Hygiene Vulnerability Scanning.** Vulnerability scanning helps secure internet-facing systems from weak configurations and known vulnerabilities and encourages the adoption of best practices. SEAs and local educational agencies (LEAs) that enroll get a weekly vulnerability scan and report, and, importantly, they are automatically enrolled in CISA's Ransomware Vulnerability Warning Pilot.

[17] https://www.nist.gov/cyberframework/online-learning/five-functions
[18] https://www.fastcompany.com/90849970/learnplatform-educators-edtech-tools
[19] Designated school officials from public and private K-12 schools that are certified to enroll international students have access to the Student and Exchange Visitor Information System (SEVIS), a national security system that incorporates FISMA security safeguards required by FISMA that go beyond the practices outlined here. Schools that use SEVIS should integrate those requirements with their other cybersecurity practices
[20] https://www.cosn.org/cosn-news/challenges-and-opportunities-of-cybersecurity-positions-in-k-12-organization-explored-in-cosn-setda-resource/

This means SEAs and LEAs get an immediate call from CISA if the scans identify a vulnerability known to be used by ransomware actors. Register for this high-impact service by emailing vulnerability@cisa.dhs.gov.

- **Check CISA's Known Exploited Vulnerabilities (KEV) catalog** to see if there are any known exploited vulnerabilities in your digital infrastructure that you can mitigate immediately.
- Sign your team up for the **CISA KEV Catalog Update Bulletin** so you receive real-time alerts when new significant vulnerabilities and mitigations arise.

Remediation of known exploited vulnerabilities is a significant first step toward a network administrator's ability to prioritize and reduce risks from the broader set of vulnerabilities that are known to the public, but not known to be exploited in the wild. Each organization's risk from a particular vulnerability is different, depending on the importance of the affected software or hardware within its network. Known exploited vulnerabilities represent the highest risk priority to organizations using the affected products. Fixing known exploited vulnerabilities is likely to produce the fastest cybersecurity results while helping your organization get ahead of future vulnerability risk.

Manage Vendor and Third-Party Risk in Procurement Process (CPGs 1.G, 1.H, 1.I)

With the proliferation of digital tools for teaching and learning, as well as for business operations, organizations must assess and manage the cyber risk posed by vendors and the supply chains on which they rely. Many SEAs and LEAs are leveraging the procurement process to address cybersecurity risks by including provisions related to incident reporting, vulnerability disclosure, and specific cybersecurity requirements. One fast and cost-effective way to reduce your organization's risk is to integrate cybersecurity requirements into the procurement process through which your organization acquires information technology goods and services, ensuring that vendors compete to demonstrate their ability to provide information and product updates for the life of the contract. Negotiating for continued support after product delivery ensures that you get more value for your IT dollar by placing contractual responsibility on your provider to help you stay ahead of supply chain risks.

NORTH DAKOTA'S WHOLE-OF-STATE APPROACH TO CYBERSECURITY

In April 2019, State Bill 2110 made North Dakota (ND) "the first state to authorize a central, shared service approach to cybersecurity strategy across all aspects of state government including state, local, legislative, judicial, K–12 education and higher education."[21] This whole-of-state approach empowered the state Chief Information Security Officer and North Dakota Information Technology (NDIT) to address third-party risk in several ways:

- **NDIT's Joint-Cybersecurity Security Operations Center (JCSOC)** protects endpoints and networks across ND and enables collaboration with at least 10 other states.[22] During the Log4j crisis,[23] JCSOC allowed ND and partners to respond at speed and scale by creating a list of 150 indicators of compromise, building detection and blocking capabilities, and helping to prevent any Log4j incidents in ND.[24]
- **Lower Insurance Costs:** Entities that adopt NDIT cybersecurity shared services receive a 4 percent reduction in cost from the North Dakota Insurance Reserve Fund, the state insurance entity.
- **Third-Party Risk Assessment:** As of July 2023, all ND state agency vendors will be required to undergo a third-party risk management assessment in order to sell products or services to any of the 57 ND state agencies.[25] NDIT provides a fast-track option for vendors with one of three recognized secure cloud services certifications—FedRAMP, StateRAMP, or HITRUST—whereby vendors are not required to complete a separate NDIT assessment.

[21] https://www.nd.gov/news/burgum-signs-legislation-creating-unified-cybersecurity-approach-north-dakota
[22] https://www.govtech.com/blogs/lohrmann-on-cybersecurity/north-dakota-ciso-shares-cyber-plans-and-priorities
[23] https://www.cisa.gov/news-events/news/apache-log4j-vulnerability-guidance
[24] https://ndlegis.gov/files/committees/67-2021/23_5183_02000_0905b.pdf
[25] https://www.ndit.nd.gov/it-services/cyber-security-governance-risk-and-compliance-services/third-party-risk-assessment

Protect

According to NIST, "the Protect Function outlines appropriate safeguards to ensure delivery of critical infrastructure services. The Protect Function supports the ability to limit or contain the impact of a potential cybersecurity event."[26] Several mitigations highlighted here reiterate the recommendations from the Cybersecurity Action Steps for the K–12 Community.

Implement Multi-Factor Authentication (CPG 2.H)

Cyber attackers are increasingly capable of phishing or harvesting passwords to gain unauthorized access to information systems. Multi-factor authentication (MFA) is a layered approach to securing online accounts and the data they contain that requires users to provide two or more authenticators to verify their identity. Users who enable MFA are significantly less likely to be hacked because even if a password is compromised, unauthorized users will not be able to meet the second authentication requirement, stopping them from gaining access to online systems and data.

Enforce Minimum Password Strength (CPG 2.B)

Despite common misconceptions, even among IT professionals, "Length is a more impactful and important factor in password strength than complexity or frequent password rotations."[27] Therefore, CISA recommends:

- **Minimum Password Length:** "Organizations have a system-enforced policy that requires a minimum password length of 15 or more characters for all password protected IT assets" given the speed and ease with which attackers' tools can crack 8-character passwords. CISA notes that this goal is "particularly important for organizations that lack widespread implementation of MFA and capabilities to protect against brute-force attacks."[28]
- **Leverage Passphrases and Password Managers:** "Organizations should consider leveraging passphrases and password managers to make it easier for users to maintain sufficiently long passwords."[29]

These recommendations do not mean all districts must move to MFA and long passwords for all users on all systems. Asking a 5-year-old who might not yet know their letters and numbers to remember and accurately type in a 15-character password and authenticate with a second factor to access an LMS would be a recipe for disaster. However, organizations can place a stronger MFA and password requirement on network administrators, for example. Administrator or network management system accounts should have password and authentication requirements and be frequently audited due to the higher risk from a compromise of these accounts. At a minimum, districts should implement the controls described herein, including MFA, for all critical systems and all users with privileged access. Ideally, districts would move to MFA and strong passwords for all staff on all systems where it is available.

ONE QUICK AND FREE ACTION YOU CAN TAKE TO PROTECT YOUR SCHOOL OR DISTRICT

Sign up for MS-ISAC's Malicious Domain Blocking and Reporting (MDBR). Designed in partnership with CISA and Akamai, the Multi-State Information Sharing and Analysis Center's (MS-ISAC) "MDBR is a cloud-based solution that uses recursive DNS [domain name system] technology to prevent IT systems from connecting to harmful web domains, helping state, local, territorial, and Tribal (SLTT) governments limit infections related to known malware, ransomware, phishing, and other cyber threats. This capability can block many ransomware infections just by preventing the initial outreach to a ransomware delivery domain."[30] This service is as close to set-it-and-forget-it as possible: it can be implemented in 15 minutes and requires almost no maintenance for SLTTs.

[26] https://www.nist.gov/cyberframework/online-learning/five-functions
[27] https://www.cisa.gov/sites/default/files/2023-03/CISA_CPG_REPORT_v1.0.1_FINAL.pdf
[28] https://www.cisa.gov/sites/default/files/2023-03/CISA_CPG_REPORT_v1.0.1_FINAL.pdf
[29] https://www.cisa.gov/sites/default/files/2023-03/CISA_CPG_REPORT_v1.0.1_FINAL.pdf
[30] https://www.cisecurity.org/ms-isac/services/mdbr

Basic Cybersecurity Training (CPG 2.I)

Train users to recognize and report phishing attempts

Since cyber attackers most frequently gain initial access by convincing users to click a phishing link or using compromised passwords, basic cybersecurity awareness training can be one of the most powerful tools for strengthening an organization's cybersecurity posture. CISA recommends at least annual training for all employees on the most common threats like phishing, business email compromise, and password security.[31] The San Diego County Office of Education (SDCOE) is an ESA that serves almost 500,000 students across 42 school districts, 129 charter schools, and 5 community college districts in Southern California.[32] Beginning with their belief that "security is everyone's responsibility,"[33] SDCOE's cybersecurity team shows how collaboration between SEAs, ESAs, LEAs, and other partners can build cybersecurity awareness capacity in school districts at scale. In response to the dramatic risk of phishing in K–12 schools, SDCOE has built and supported Red Herring, which is "a system that sends simulated phishing emails and tracks the actions taken by the targeted users." Designed as part of a comprehensive cybersecurity awareness program, Red Herring allows districts to synchronize users from commonly used systems, leverage existing email templates, or customize their own emails and landing pages.

Develop and Exercise a Cyber Incident Response Plan (CPG 2.S)

The single most important thing a school district can do to prepare for a cyber incident is develop and exercise an incident response plan (IRP). IRPs articulate how to leverage the people, processes, and tools within a district before, during, and after an actual or potential cybersecurity incident.

K12 SIX ESSENTIAL CYBER INCIDENT RESPONSE RUNBOOK

To help K–12 leaders jumpstart their incident response plans, K12 Security Information Exchange (K12 SIX)—a cyber threat information sharing hub for K–12 organizations—partnered with K–12 cybersecurity leaders to develop the ***K12 SIX Essential Cyber Incident Response Runbook***. IRPs in general, and the *Runbook* specifically, can help prepare schools to respond to a cyber incident by answering questions such as:

- Who is part of our cyber incident response (IR) team and what do they do during an incident?

  Roles can include IR Team Leader, IR Team Administrator, First Responder, IR Team Lead Investigator, and Communications/PR

- How do we declare a potential cyber incident and mobilize the IR team?
- Who are the key contacts (internal and external)? How do we reach them? Do we have alternative communication channels in case internal systems are compromised or offline?
- How do we alert executive leadership, legal counsel, law enforcement, etc.? Who do we call first, second, third, etc.?
- How do we plan to notify stakeholders and affected parties, in compliance with our legal obligations and policy?

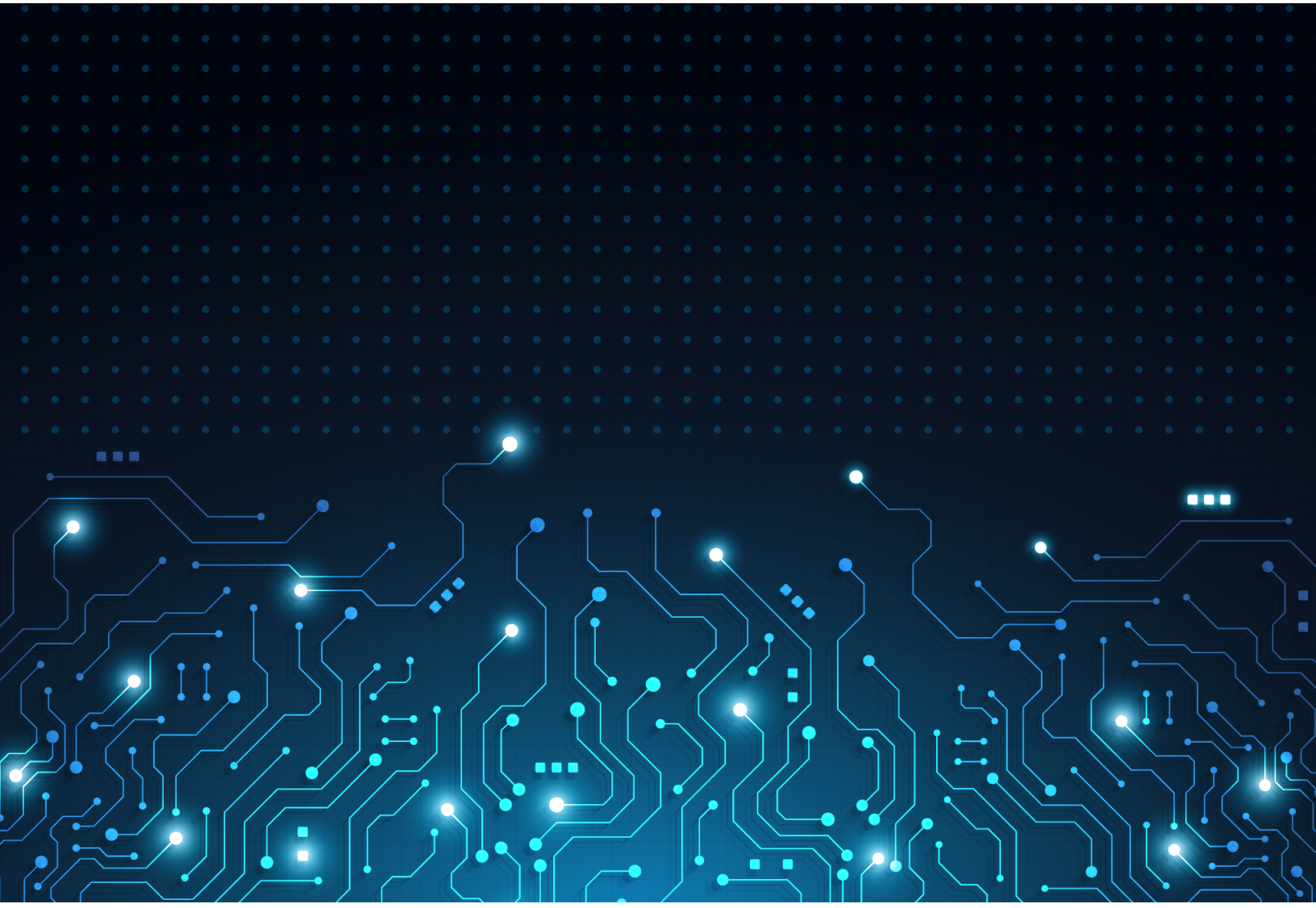
[31] https://www.cisa.gov/sites/default/files/2023-03/CISA_CPG_REPORT_v1.0.1_FINAL.pdf
[32] https://www.sdcoe.net/about-sdcoe
[33] https://www.sdcoe.net/administrative-services/technology/cybersecurity

INTEGRATING CYBERSECURITY WITH EMERGENCY OPERATIONS PLANNING

Cybersecurity should be considered within the larger framework of school and district emergency preparedness activities that address security, safety, and emergency management.

SchoolSafety.gov: Launched in 2020 as a collaboration between CISA, ED, DOJ, and HHS, schoolsafety.gov "empowers districts and schools to improve safety and security." Growing out of the work of the Federal School Safety Clearinghouse, the free site is a one-stop shop for "evidence-based content and recommended best practices to keep schools safe" across topics like emergency planning, physical security, and cybersecurity.

Readiness and Emergency Management for Schools (REMS) Technical Assistance (TA) Center: Administered by ED's Office of Safe and Supportive Schools, REMS TA Center builds emergency preparedness capacity for schools and districts in both the physical security and cybersecurity domains. The REMS TA Center website includes an online course on "Cybersecurity Considerations for K–12 Schools and School Districts" as well as podcast episodes about integrating cyber safety into emergency operations plans (EOPs).



Detect

Cybersecurity is a team sport, so don't go it alone. When it comes to detecting relevant threats and tactics, techniques, and procedures (TTPs), here are some of the highest-impact actions you can take:

Join an Information Sharing and Analysis Center (ISAC)

Join the MS-ISAC: MS-ISAC is a CISA-funded Information Sharing and Analysis Center (ISAC) operated by the Center for Internet Security designed to serve as the central cybersecurity resource for the nation's state, local, territorial, and Tribal (SLTT) governments, including educational institutions. Members receive direct access to a suite of services and informational products including cybersecurity advisories and alerts, vulnerability assessments, incident response support, secure information sharing, tabletop exercises, a weekly malicious domains/IP report, and more. To learn more about the MS-ISAC program, email directly at info@msisac.org or visit their website at at www.cisecurity.org/ms-isac.

Many leaders find additional value in joining no-cost and low-cost national, state/regional, or education-focused information sharing groups that connect them with other leaders in their area or sector. For example:

- Many states have established their own ISACs. For example, the North Carolina Department of Information Technology has developed an integrated approach that includes mandatory incident reporting, information sharing via NC-ISAC, and incident response support, which is discussed in more detail in the *Respond* section below.
- **K12 SIX** is a non-profit that operates an ISAC "for the K-12 education sector, facilitating the sharing of actionable threat intelligence with its membership."[34]
- **Infragard** is a partnership between the FBI and "members of the private sector for the protection of U.S. Critical Infrastructure. Through seamless collaboration, InfraGard connects owners and operators within critical infrastructure to the FBI, to provide education, information sharing, networking, and workshops on emerging technologies and threats."[35]

In addition to providing accessible and equitable pricing for broadband to 100 percent of the school districts in Connecticut, the Connecticut Education Network (CEN) includes a number of cybersecurity services at no additional cost. CEN provides Distributed Denial of Service (DDoS) monitoring and mitigation protections, inline and remote Children's Internet Protection Act (CIPA) filtering for all K–12 districts and libraries (which expanded to include 1:1 device initiatives during emergency remote learning and throughout the pandemic), and DNS firewall.[36]

[34] https://www.k12six.org/about
[35] https://www.infragard.org/
[36] https://www.setda.org/master/wp-content/uploads/2019/04/Broadband-State-Leadership-2019-Connecticut.pdf

Respond

Given the trends in cyber incidents in K–12 school districts, district leaders need to plan for when, not if, a cyber incident will impact their organization. In addition to developing an incident response plan (discussed in the Protect section), the most important step to mitigate cyber risk in the response function is **connecting to dedicated incident response resources** at the state and regional levels.

Cyber Incident Response is a Team Sport

There are many federal, state, regional, and local resources to support you as you navigate what may be one of the most challenging experiences of your career. In terms of federal support for incident response, your two most important points of contact are your local FBI field office and your CISA regional Cyber Security Advisor. If you are not sure how to find CISA or FBI help locally, contact your CISA regional office or local FBI field office.

Across the country, state agencies, universities, and non-profits are finding innovative ways to help school districts respond to cyber threats. Some examples include:

- **North Carolina's Joint Cybersecurity Task Force:** North Carolina's whole-of-state approach provides a powerful example that combines information sharing, mandatory incident reporting, and real-time incident response in support of K–12 schools. In January 2021, North Carolina built a Joint Cybersecurity Task Force that includes the FBI, National Guard, SEA, and school districts.[37] The task force is authorized by the governor and the legislature to mobilize the National Guard and deploy a strike force to support districts immediately upon learning of a cybersecurity incident, which all school districts and local governments are required to report based on the state's new incident reporting law. "The IT Strike Team is a group of volunteers and members of the North Carolina Local Government Information Systems Association (NCLGISA), an association of local government IT professionals. Strike team members volunteer their time and skills and, along with the National Guard, serve as boots on the ground to provide on-scene response and recovery services."[38]

- **Texas State Government and State University Collaboration:** In Texas, a state-funded Regional Security Operations Center (RSOC) pilot program provides real-time network security monitoring and incident response support to local governments, including school districts. Built on a partnership between the Texas Department of Information Resources and Angelo State University, this model enables local highly skilled staff and students to protect the defensibility and resilience of their communities' networks, provides students with real-world experience in cybersecurity career pathways, and keeps the cost of the program down.[39]

- **Toward a Cyber 311 Hotline and Community Cyber Defense:** Non-profit organizations, universities, local governments, and volunteers across the country have been stepping up to protect K–12 school districts and other organizations below the "cybersecurity poverty line" (CPL) due to "insufficient IT budget, expertise, capability, or influence."[40] One innovative approach envisions a "Cyber 311" service that can offer emergency help to local school districts and businesses experiencing a cybersecurity incident.[41] Although a fully functional "Cyber 311" may be several years away, universities[42] participating in the Consortium of Cybersecurity Clinics are opening "Cyber Clinics" to support institutions below the CPL now. Borrowing from the law school clinic model, where law school students support the local community with pro bono legal services,

[37] https://www.nascio.org/wp-content/uploads/2021/08/NC-JCTF-NASCIO-Nomination-2021-Cyber.pdf
[38] https://www.nascio.org/wp-content/uploads/2021/08/NC-JCTF-NASCIO-Nomination-2021-Cyber.pdf
[39] https://dir.texas.gov/news/dir-partners-angelo-state-university-pilot-regional-security-operations-center
[40] https://www.atlanticcouncil.org/content-series/buying-down-risk/cyber-poverty-line/
[41] https://www.wired.com/story/ut-austin-cybersecurity-clinic-311/
[42] As of June 2023, consortium members included University of California, Berkeley's Center for Long-Term Cybersecurity and School of Information, Massachusetts Institute of Technology, Indiana University, the University of Alabama, the University of Georgia, Rochester Institute of Technology, Stillman College, Columbia University School of International and Public Affairs, University of Nevada, Las Vegas, University of Texas at Austin, and University of Texas at San Antonio.

cyber clinics like the pilot project Applied Cybersecurity Community Clinic at the University of Texas at Austin seek to provide organizations below the CPL with cybersecurity protection and response support.[43] Bridgewater State University in Massachusetts is taking the additional step of partnering with a consortium of professional cybersecurity experts to staff a 24/7 security operations center with the support of cybersecurity students to make a version of Cyber 311 hotline a reality in fall 2023.[44]

Run a Tabletop Exercise with your District Leadership Team (CPGs 1.F, 4.A)

As a district leader focused on buying down cybersecurity risk, there is no bigger bang for your buck than running a 60–90-minute tabletop exercise with your executive leadership team. A tabletop exercise is a scenario-based session where members of a team practice and talk through their roles and responsibilities during a cybersecurity incident. In contrast to the high-stress, high-risk experience of an actual incident, the tabletop exercise is an opportunity to build a culture of cybersecurity awareness in a collaborative and collegial environment. The goal is to identify cyber risks and gaps in current processes, provide a space for the leaders around the table to develop solutions that mitigate those risks and close those gaps, and build muscle memory to make incident response and recovery a part of organizational culture. Drills and exercises offer a way of making infrastructure visible to the community so everyone can understand their role in protecting it and what to do in case it fails.

CISA and ED have developed K–12-specific tabletop exercises that you can use immediately or modify to meet specific needs. CISA's K–12 Schools Tabletop Exercise Package features a scenario where a threat actor targets district employees through phishing emails. Ransomware compromises the computer system with multiple impacts including exfiltration of students' PII, loss of school HVAC system control, and media inquiries.[45] In the REMS-TA Cybersecurity Tabletop Exercise, you should imagine that you are a member of your school's emergency planning team and that you have access to only the resources and systems you currently have in place. You will discuss your response to a hypothetical cybersecurity incident, specifically a data breach that occurs because of malware.[46]

[43] https://www.strausscenter.org/cybersecurity/apply-here-cyber-clinic/
[44] https://www.bridgew.edu/about-us/news-events/Press-Release-03-02-2023-Bridgewater-State-University-launches-first-of-kind-cybersecurity-program-in-Massachusetts
[45] https://www.cisa.gov/resources-tools/resources/cybersecurity-scenarios
[46] https://rems.ed.gov/docs/CybersecurityTabletop_508C.pdf

Recover

People only tend to notice infrastructure when it's not working. When it comes to recovery, there is one high-impact action every school district should take: practice restoring your critical systems from backups. According to NIST, "The Recover Function identifies appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident. The Recover Function supports timely recovery to normal operations to reduce the impact from a cybersecurity incident.[47]

Perform and Test Backups (CPGs 2.R, 5.A)

To ensure continuity of learning[48] and operations in the event of a cyber incident or other emergency, many school districts have implemented processes for backing up their critical data and systems. However, it is much less common for districts to practice fully restoring systems from backups. So, unfortunately, when a district gets hit with a ransomware attack that encrypts their network, even though they may have backups to help them continue operations and mitigate impact, those backups may not actually work in practice. To avoid this pitfall and reduce the impact of ransomware and other damaging attacks, CISA recommends:[49]

> Identify data that is critical to continued operations of the K–12 organization and implement backup solutions that are separated from the operational network. Conduct recurring real-world tests to ensure that data can be readily restored from backups. Where applicable, consider free tools such as Windows Auto-Backup[50] and Google Backup & Sync.[51] 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.

Being able to restore critical digital infrastructure from backups has helped school districts avoid disruptions to learning and operations as well as protected them from having to pay ransomware actors to resume operations. When Athens Independent School District in Texas was hit with ransomware in July 2020, they quickly restored their most important database, including student records, from redundant backups and avoided paying the ransom.[52] When Wilkes-Barre Career and Technical Center in Pennsylvania was hit with ransomware on a payroll server in March 2023, they were able to make payroll after restoring from a backup in secure cloud storage. While the school had to shut down its computer and Wi-Fi network to contain the incident, they leveraged flexible instruction days to provide remote instruction to their roughly 750 students via Google Classroom, which was unaffected by the incident.[53] For more on backups, check out the K12 SIX Essential Cybersecurity Protections, which include guidance on offline, immutable backups and strategies for implementing backup processes.

[47] https://www.nist.gov/cyberframework/online-learning/five-functions

[48] Schools in such situations would have to consider the DHS restrictions on remote learning for any international students and any necessary reporting to DHS's Student and Exchange Visitor Program (SEVP) about their emergency situation. Once the COVID flexibilities are fully lifted at the beginning of the Fall 2023 semester, the regulatory restrictions on the number of hours that can be done via remote learning/online classes will resume, and a school with international students will need to consider how to navigate those regulations in implementing any remote/online learning schedules.

[49] https://www.cisa.gov/online-toolkit-partnering-safeguard-k-12-organizations-cybersecurity-threats

[50] https://support.microsoft.com/en-us/windows/backup-and-restore-in-windows-352091d2-bb9d-3ea3-ed18-52ef2b88cbef

[51] https://support.google.com/drive/answer/7638428

[52] https://www.athensreview.com/news/athens-isd-recovers-data-and-rejects-cyberattackers/article_ae6bf366-d367-11ea-af3b-a72601a99900.html

[53] https://www.govtech.com/education/higher-ed/tech-school-prevented-catastrophe-with-antivirus-backup

What Vendors Can Do

Vendors should follow all recommendations for school districts provided throughout this brief, and districts should consider requiring vendors to do so. In alignment with the March 2023 National Cybersecurity Strategy, vendors should make investments that strike a "careful balance between defending ourselves against urgent threats today and simultaneously strategically planning for and investing in a resilient future."[54]

For immediate steps that vendors can take to improve customer defensibility today, see CISA CPG[55] recommendations, such as:

- **Enforce a minimum password length of 15 characters by default (CPG 2.B).** This small change will improve customers' cybersecurity posture at no cost. This change will also require customers to affirmatively choose to make their organizations less secure if they choose a shorter minimum password length.
- **Enforce MFA on critical systems and privileged accounts by default (CPG 2.H).** Enforcing MFA by default on privileged accounts dramatically improves the defensibility and resilience of customers at no cost. It also requires customers to affirmatively elect to make their organizations less secure if they choose to disable MFA on critical systems and privileged accounts. This recommendation is especially important on systems that store student and staff PII such as the SIS and ERP, as well as systems critical to the continued operations of the organization such as the VPN, email, IAM, and server infrastructure.
- **Publish a vulnerability disclosure policy (CPG 4.B).** Allow security researchers to report security vulnerabilities to your organization, strengthening the security of your organization and your relationship with security researchers. A vulnerability disclosure policy should authorize testing against all products offered by the vendor, provide legal safe harbor that authorizes testing under the policy, and allow public disclosure of vulnerabilities after a set timeline.

For more strategic investments in a resilient future for their customers and themselves, today, vendors should:

- **Build Secure-by-Design:** Since SEAs and LEAs rely on the private sector for much of their critical digital infrastructure and most SEAs and LEAs leverage the same handful of vendors for their most critical systems (SISs, ERPs), vendors can have a powerful impact on improving the defensibility and resilience of the sector. We have seen that in the K–12 education market, often a few vendors are uniquely situated to impact thousands of districts at a time by taking concerted actions to make their systems secure by design. For industry partners, the best place to start is CISA's April 2023 guidance document Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-by-Design and -Default. Key actions include:

[54] https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/02/fact-sheet-biden-harris-administration-announces-national-cybersecurity-strategy/

[55] https://www.cisa.gov/sites/default/files/2023-03/CISA_CPG_REPORT_v1.0.1_FINAL.pdf

» taking ownership of security outcomes for customers, such as including key security features by default, at no additional charge;

» embracing radical transparency, such as publishing a Secure-by-Design roadmap; and

» building organizational structure to accomplish these goals.

- **Ensure that systems and software are both accessible and secure**: Secure systems and software should conform with key accessibility-related frameworks and standards and allow interoperability with assistive technologies that may be in use by students and school personnel.
- **Third-Party Risk Assessment**: By getting a certification from a recognized authority, vendors demonstrate their willingness and ability to provide cyber risk assurance to SEAs, ESAs, and LEAs. While there are several options, they all take a similar approach. To contract with a particular entity—federal agency, state agency, LEA—a cloud service provider must obtain certification from outside assessment organizations who perform initial (and often periodic) security assessment. Examples include:

» **FedRAMP**: "The Federal Risk and Authorization Management Program (FedRAMP®) was established in 2011 to provide a cost-effective, risk-based approach for the adoption and use of cloud services by the federal government. FedRAMP empowers agencies to use modern cloud technologies, with an emphasis on security and protection of federal information."[56]

» **StateRAMP**: Expanding on the idea of FedRAMP, StateRAMP "uses a network of outside assessment organizations to rate the security of cloud vendors" doing business with state and local governments.[57]

[56] https://www.fedramp.gov/program-basics/
[57] https://statescoop.com/stateramp-cloud-security-k12-university-north-carolina/

Conclusion

Organizational cyber risk management aligns people, processes, and tools, to effectively identify, detect, protect, respond to, and recover from cybersecurity incidents. As with fire safety for our physical school buildings, superintendents and IT leaders must strive to prevent cyber incidents with digital infrastructure that is defensible and resilient at the perimeter. Systems block and filter malicious traffic and emails, IT staff patch known exploited vulnerabilities on internet facing hardware and software, and system administrators enforce strong passwords and MFA to prevent unauthorized access to accounts, systems, and data. However, leaders know it's not a question of if, but when, a malicious actor will evade their perimeter defenses and gain unauthorized access. To mitigate harm and enable resilient response and recovery, districts use automated tools for detection, train users what threats to look for and how to report them, and practice implementing incident response plans. Cybersecurity fire drills combined with the low-cost, high-impact recommendations highlighted in this brief have the power to dramatically reduce the cybersecurity risk for SEAs, ESAs, and LEAs across the country.