

Cybersecurity for K-12 Schools and School Districts: Developing a Cyber Annex

READINESS AND EMERGENCY MANAGEMENT FOR SCHOOLS TECHNICAL ASSISTANCE CENTER

School districts and individual schools must be prepared for a wide variety of threats and hazards—under varied circumstances, in all settings, and at all times. Safe, secure, resilient, and accessible education system infrastructure, both physical and digital, is an essential factor for success. Yet the digital infrastructure in our nation’s K-12 schools is increasingly under threat from malicious cyber actors.

Although cybersecurity incidents were not infrequent prior to the COVID-19 pandemic, threat actors have taken advantage of the increased post-pandemic integration of and reliance on digital infrastructure and educational technology to target K-12 institutions, often with highly disruptive and costly results. The Multi-State Information Sharing and Analysis Center’s (MS-ISAC) recent [K-12 Report](#) finds that having a wealth of student data, combined with resource constraints, makes K-12 institutions particularly attractive targets for cyber threat actors, with 29 percent of MS-ISAC’s K-12 member organizations reporting having experienced a cybersecurity incident. The K12 Security Information Exchange’s (K12 SIX) 2022 [State of K-12 Cybersecurity: Year in Review](#) reports that from 2016 to 2021, schools in nearly every state in the country were victims of a cyberattack, with the frequency of attacks increasing from an average of about 200 a year in 2016 and 2017 to an average of about 300 a year from 2018 to 2021. The report also finds that while larger and wealthier school districts are more likely to experience cybersecurity incidents, smaller school districts, which may be more vulnerable to cyberattacks and may require more substantial resources and support to recover from cybersecurity incidents, are less likely to report them.



Cybersecurity incidents have serious short- and long-term impacts on the continuity of operations of educational agencies and can result in business operations disruption, the exposure of sensitive school safety information, monetary loss, learning loss, and the compromise or loss of sensitive student and staff data. For example, a ransomware attack can result in class cancellations and school closures; loss of access to curricula and educational tools and technology; extortion of school funding; monetary losses caused by the time and resources needed to respond and recover; loss of confidential and sensitive information, including Social Security numbers; and the loss of school community trust.

Federal legislators are responding quickly to support school districts and individual schools as they weather attacks on their digital infrastructure. In 2021, Congress passed the K-12 Cybersecurity Act, mandating that

Threats Facing K-12 Digital Infrastructure

Multiple reports—including CISA's *Protecting Our Future*, K12 SIX's 2022 *State of K-12 Cybersecurity: Year in Review*, and MS-ISAC's *K-12 Report*—identify the most common types of threats to K-12 digital infrastructure:

- **Ransomware Attacks.** Ransomware is a form of malware—*malicious software designed to steal data and damage or destroy computers and computer systems*. During ransomware attacks, perpetrators attempt to or successfully exfiltrate data and encrypt users' files as leverage to extort money from them. Frequently delivered through phishing or spoofing scams, malware uses social engineering tactics to tempt users to click on a link, which then downloads malicious software that infects their computers or systems. Once a computer or system is infected, the perpetrator of the malware attack threatens to publish sensitive data or permanently block access to files unless the victim pays a ransom.
- **Data Breaches.** A data breach is a leak or spill of sensitive, protected, or confidential data from a secure environment to an insecure environment. The data are then copied, transmitted, viewed, stolen, or used in an unauthorized manner. Data breaches often occur with confidential information, such as students' records. This information may be inappropriately viewed or used by an individual who should not have access to it. The two most frequently reported types of data breaches for school districts and individual schools are data breaches involving student information and data breaches involving staff and school community member information.
- **Business Email Compromise (BEC) Scams.** These attacks are a targeted form of phishing known as spear phishing. Phishing is the act of sending an email in which one falsely claims to be a legitimate organization to deceive the recipient into visiting a fake Website and divulging sensitive information (e.g., passwords, credit card numbers, or bank account information). BEC scams are a type of email cybercrime in which perpetrators impersonate current and trusted members of an organization to trick victims into providing sensitive information or money.

the Cybersecurity and Infrastructure Security Agency (CISA) evaluate and report on the cybersecurity threats facing the nation's K-12 digital infrastructure and offer recommendations and best practices. The resultant report, [Protecting Our Future: Partnering to Safeguard K-12 Organizations From Cybersecurity Threats](#) (*Protecting Our Future*), offers information on the most common types of cyber threats, provides strategies on incorporating the [National Institute of Standards and Technology \(NIST\) Cybersecurity Framework \(CSF\)](#) into cybersecurity plans, and shares recommendations for bolstering educational digital infrastructure and planning for cybersecurity incidents.



Just as core planning teams at school districts and individual schools work to ensure that all physical threats and hazards are identified and prepared for using an all-hazards approach, so too should core planning teams address cybersecurity in their emergency management planning efforts. This means that they should assess their digital infrastructure; identify cybersecurity risks and vulnerabilities; collaborate with key cybersecurity partners; develop high-quality, comprehensive school emergency operations plans (EOPs) that include a Cyber Annex; and exercise their plans regularly.

This fact sheet describes the most common types of cyber threats currently facing school districts and individual schools; offers strategies for preparing for cyber threats; shares actionable recommendations that key school community groups can take before, during, and after a cybersecurity incident; and provides information on how to incorporate cybersecurity considerations into every step of EOP development.

Key Cybersecurity Frameworks and Considerations

In support of school districts and individual schools as they work to strengthen, augment, and sustain K-12 digital infrastructure, the U.S. Department of Education's Office of Educational Technology (OET) released several foundational guidance documents.

The second in a series, the [K-12 Digital Infrastructure Brief: Defensible & Resilient \(Defensible & Resilient\)](#), issued in partnership with CISA in 2023, describes a threat-informed, risk-based approach to cybersecurity. The brief provides recommendations that complement the NIST CSF and builds on the 2017 OET brief, *Building Technology Infrastructure for Learning* report, and offers key considerations and high-impact actions that school districts and individual schools can take to mitigate, prevent, protect the school community from, respond to, and recover from cybersecurity incidents. Key considerations include:

- **Enhance Continuous Risk Management.** Cybersecurity involves a continuous process of managing risk. School districts and individual schools can address the inherent insecurity in digital infrastructure by adopting a proactive approach to managing cybersecurity risks.
- **Create Analogies for Understanding.** Drawing analogies from the physical world and leveraging lessons learned can assist educators, school leaders, students, staff members, and the school community in understanding and effectively addressing cybersecurity challenges.



- **Distributed Denial-of-Service (DDoS) Attacks.** DDoS attacks are cyberattacks in which a server is deliberately overloaded with requests until access is temporarily or permanently disrupted. These attacks halt the normal functioning of a targeted server by flooding it with superfluous traffic until the network is overwhelmed and a service outage occurs.
- **Website and Social Media Defacement.** Website and social media defacement involves incidents in which unauthorized changes, such as the publication of inappropriate or offensive images or language, are published to a school or school district Website or social media account.
- **Online Class and School Meeting Invasions.** Online class and school meeting invasions are situations in which a perpetrator accesses an online voice or video platform without authorization for the purpose of disruption. Perpetrators of invasion often expose victims to hate speech; offensive images, sounds, and videos; and threats of violence.

NIST CSF and High-Impact Action Items

The [NIST CSF](#) organizes cybersecurity activities at their highest level. They are listed below, along with high-impact action items.

- **Identify.** Conduct an inventory of cyber assets and an assessment of cybersecurity risks.
- **Protect.** Implement multifactor authentication (MFA) and enforce minimum password strength.
- **Detect.** Join an information sharing and analysis center (ISAC).
- **Respond.** Exercise your Cyber Annex and cyber incident response plan and practice [CISA's tabletop exercise for K-12 schools](#) to strengthen response capacity before an incident occurs.
- **Recover.** Practice restoring critical systems from backups so that those responsible with this task during an incident are comfortable with the process.

- **Prioritize Critical Risks and Implement High-Impact Mitigation Strategies.** Federal guidance recommends focusing on the most impactful mitigation measures first, such as implementing MFA, enforcing minimum password strength, recognizing and reporting phishing attempts, and keeping software updated by patching known exploited vulnerabilities.
- **Build Resilience for Cyber Incidents.** Planning teams can build resilience by developing and exercising a Cyber Annex and a cyber incident response plan and by running cybersecurity tabletop exercises with school leadership.
- **Engage Vendors to Enhance Security.** School districts and individual schools can encourage vendors to strengthen investments and systems that enhance the defensibility and resilience of K-12 digital infrastructure. Vendors should invest in secure design principles, obtain cyber risk assurance certifications, and establish security vulnerability disclosure practices.



Preparing for Threats to K-12 Digital Infrastructure

School districts and individual schools can take a variety of actions to prevent, protect the school community from, mitigate the effects of, respond to, and recover from cyber threats.

Before a Cybersecurity Incident

To protect K-12 digital infrastructure as part of an overall preparedness program, schools can do the following:

- **Develop and promote policies on responsible use.** Before students, teachers, or staff *members* access the school district's or individual school's networks and systems, they should be aware of any policies, rules, and laws regarding their use. The whole school community can be required to accept a responsible use policy. Information technology (IT) staff *members* should also be aware of local, state, and Federal regulations about information security, privacy, and storage of *sensitive information*.

- **Assess current digital infrastructure.** Conducting a cybersecurity risk assessment can help planning team members comprehensively understand the cybersecurity landscape to which they are exposed and can support the development and enhancement of a high-quality Cyber Annex.
- **Store data securely to ensure that the whole school community's data are kept private and to comply with the Family Educational Rights and Privacy Act (FERPA).** Both CISA's *Protecting Our Future* report and OET's *Defensible & Resilient* report recommend that school districts and individual schools minimize the burden of security by migrating data from on-premises IT systems to cloud-based services. Further, the guidance recommends prioritizing high-impact targets, such as identity services and mail systems, for migration to the cloud. Schools can also benefit from regularly backing up their data in case of accidental or deliberate corruption or destruction of data.
- **Create firewalls and an approved list of individuals who have access to the school district's or individual school's networks and systems.** Regularly review this list to ensure that only those individuals who have permission to access the systems can do so.
- **Monitor networks continuously to reduce the risk from cyber threats.** School districts and individual schools can increase their monitoring, detection, and protection capacity by connecting to dedicated cybersecurity incident response resources at the local, state, and regional levels.

- **Consider purchasing cyber insurance.** Understand how your education agency’s cyber posture informs your eligibility for and the cost of cyber insurance. Insurers increasingly expect that organizations demonstrate cyber prevention efforts including network security (i.e. MFA, constant scanning, etc.), data protection, training, and staffing.
- **Practice exercising response plans and the Cyber Annex, and practice restoring data from backups.** By practicing plans, core planning teams and all those involved in the plans have the opportunity to strengthen their capacity to respond effectively during an incident and identify vulnerabilities or gaps within the plans.

During a Cybersecurity Incident

Once an incident or a suspected incident occurs, actions should include the following:

- **Report the cybersecurity incident.** In most cases, the first point of contact will be the school district’s or individual school’s IT manager or team.
- **Limit the damage to digital infrastructure.** School technical and leadership teams can respond quickly to limit the damage and preserve sensitive information. Decisions may also need to be made about whether to request external assistance and, if so, from whom, such as from the school district; a local, state, or Federal government computer incident response team; or a private vendor.
- **Notify law enforcement.** Law enforcement should be notified as soon as possible during an incident, as well as any individuals whose personal information may have been compromised. A report can be made to:
 - The FBI, via a [field office cyber task force](#), its [Internet Crime Complaint Center](#), or its National Cyber Investigative Joint Task Force (cywatch@ic.fbi.gov);
 - CISA, via its [Emergency Communications Coordinators and Cyber Security Advisors](#) or the [Computer Emergency Readiness Team \(US-CERT\)](#); or
 - The National Cybersecurity and Communications Integration Center (nccic@hq.dhs.gov).

After a Cybersecurity Incident

Once the incident has been contained, recovery may be needed for people, policies, and technology—all of which are interconnected. The following actions can support recovery:

- **Restore continuity of operations as quickly as possible.** Essential functions—such as business services, communication systems, and computer systems—should be restored as soon as possible to limit further school closures and to avoid further learning disruptions.



- **Identify victims and connect them to relevant support services.** If student, educator, staff, or school community data have been breached, timely and effective communication of available resources and support services fosters continued trust within the school community and aids in individual and school community recovery.
- **Identify and address any impacts to digital infrastructure.** Assess any temporary or permanent damage to digital infrastructure, and evaluate and patch the system for any exploited vulnerabilities.
- **Conduct an after-action review and create an after-action report.** There is no better time to conduct an after-action review and create an [after-action report](#) than just after an incident, while the experience is still fresh. Shortly after a cybersecurity incident, the planning team can convene and evaluate its response, document the gaps and strengths in its current Cyber Annex, and enhance any sections where issues arose.

Incorporating Cybersecurity Into EOP Development

The [Guide for Developing High-Quality School Emergency Operations Plans](#) and [The Role of Districts in Developing High-Quality School Emergency Operations Plans](#) set forth a cyclical six-step planning process for developing comprehensive school EOPs. This includes the creation and maintenance of a Cyber Annex that contains goals, objectives, and courses of action for before, during, and after a cyber incident. By incorporating cybersecurity into EOP development, the core planning team can also better prepare for cross-cutting operational actions or functions, such as continuity of operations, communications and warnings, security, and recovery. Cybersecurity considerations may also be incorporated into functional annexes within the EOP. When developing a Cyber Annex, the core planning team can progress through the six-step planning process as follows.

Step 1: Form a Collaborative Planning Team

A wide-ranging, collaborative planning team—including school personnel, school district staff members, community partners, school administrators, students, and parents—is established. The core planning team should also include IT specialists, school district technology leaders, law enforcement officers, and other relevant stakeholder groups that can contribute cybersecurity expertise.

Step 2: Understand the Situation

The core planning team identifies all possible threats and hazards that the school community may face using a variety of data sources. One source includes school and school district assessments, such as site assessments that include examining education agency networks

and systems and [cybersecurity risk assessments](#). Other sources are input from local, state, and Federal agencies and input from the school community. For example, [CISA's Capacity Enhancement Guide](#), [Phishing-Resistant MFA Fact Sheet](#), and [Partnering to](#)

[Safeguard K-12 Organizations Online Toolkit](#) all support better understanding of current threats against networks and systems. Once identified, the planning team evaluates the risks and vulnerabilities and prioritizes threats and hazards.

Step 3: Determine Goals and Objectives

The planning team selects threats and hazards to address in the EOP and creates goals and objectives for before, during, and after an incident. Goals include broad, general statements that describe a desired outcome, whereas objectives are specific, measurable actions that are necessary to achieving the goals. School districts and individual schools may benefit from referring to the NIST CSF, the *Protecting Our Future* report, [CISA's Cross-Sector Cybersecurity Performance Goals](#), and *Defensible & Resilient* to find inspiration and guidance for establishing relevant, impactful, and actionable goals and objectives that address cyber threats to schools' digital infrastructure.

Step 4: Plan Development (Identifying Courses of Action)

Goals and objectives form the foundation for Step 4, which involves developing a course of action for each identified objective. A course of action describes the exact tasks that will be completed to meet an objective and includes criteria for determining how, when, and by whom each response will be implemented under a variety of circumstances. After completing Step 4, the planning team will have clearly defined goals, objectives, and courses of action that will be the content of the Cyber Annex.



Step 5: Plan Preparation, Review, and Approval

A draft of the EOP is written and circulated to obtain feedback from those responsible for implementing the document. During Step 5, the plan will be formatted, reviewed for compliance with applicable laws, and approved by school leadership and relevant stakeholders. The Cyber Annex is usually found in the [Threat- or Hazard-Specific Annexes](#) section, but there is no single correct EOP format. The core planning team should review the Cyber Annex against policy and guidance put forth from local, state, and Federal agencies.

Relevant Federal Laws

Every Cyber Annex should be reviewed for compliance with the following Federal laws:

- [Family Educational Rights and Privacy Act \(FERPA\)](#)
- [Protection of Pupil Rights Amendment \(PPRA\)](#)
- [Children's Internet Protection Act \(CIPA\)](#)
- [Children's Online Privacy Protection Act \(COPPA\)](#)

Step 6: Plan Implementation and Maintenance

School districts and individual schools implement the activities described in the EOP, including conducting training or professional development for those who have a role or responsibilities in an emergency. This step also involves exercising the plan via tabletop exercises, drills, functional exercises, and full-scale exercises, as well as reviewing, revising, and maintaining the plan after incidents or exercises. The planning team may find it beneficial to practice the Cyber Annex by conducting a cyber tabletop exercise from the [REMS TA Center's Emergency Exercises Training Package](#) or [CISA's tabletop exercise for K-12 schools](#). As new cyber threats are constantly emerging, the planning team may decide to review the Cyber Annex more frequently than other annexes within the EOP.



Conclusion

Safety leaders navigating the current K-12 cybersecurity landscape are facing whole-community challenges that require comprehensive whole-community solutions. School district leaders, school IT specialists, educators, students, parents and caregivers, state leaders, vendors and service providers, and the entire school community play key roles in maintaining safe, accessible, resilient, and effective K-12 digital infrastructure.

Resources

Further Reading – REMS TA Center

- [Cyber Safety Considerations for K-12 Schools and School Districts](#), Fact Sheet
- [K-12 Online Classrooms: Emergency Management Planning for All Settings](#), Fact Sheet
- [Addressing Adversarial and Human-Caused Threats That May Impact Students, Staff, and Visitors](#), Web Page

Training Opportunities – REMS TA Center

- [Emergency Exercises Training Package: Cybersecurity Tabletop Exercise](#), Specialized Training Package
- [Integrating Cybersecurity Into School Emergency Operations Plans](#), Specialized Training Package

- [Cybersecurity Considerations for K-12 Schools and School Districts](#), Online Course
- [Understanding the Role of Information Technology Specialists in Supporting School Safety Before, During, and After an Emergency](#), Webinar
- [Creating, Revising, and Enhancing Emergency Operations Plans to Support Cyber Safety](#), Podcast Series

Further Reading – Digital Educational Technology

[Reimagining the Role of Technology in Education: 2017 National Education Technology Plan Update](#), Publication (U.S. Department of Education, Office of Educational Technology)

- [School Leader Digital Learning Guide](#), Publication (U.S. Department of Education, Office of Educational Technology)
- [K-12 Digital Infrastructure Brief: Privacy Enhancing, Interoperable, and Useful](#), Publication (U.S. Department of Education, Office of Educational Technology)


- [K-12 Digital Infrastructure Brief: Adequate and Future Proof](#), Publication (U.S. Department of Education, Office of Educational Technology)


Further Reading – Cyber Mitigation


- [Cybersecurity Action Steps for the K-12 Community](#), Publication (SchoolSafety.gov)
- [Malicious Domain Blocking and Reporting \(MDBR\)](#), Web Page (Multi-State Information Sharing and Analysis Center)
- [Essential Cybersecurity Protections for the 2022-2023 School Year: What K-12 Leaders Need to Know](#), Publication (K12 Security Information Exchange)


Further Reading – Cyber Recovery


- [Security Advisors](#), Web Page (U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency)
- [Essential Cyber Incident Response Runbook](#), Publication (K12 Security Information Exchange)



 [\(855\) 781-REMS \(7367\)](tel:(855)781-REMS(7367))

 info@remstacenter.org

 [@remstacenter](https://www.instagram.com/remstacenter)

 <https://remstacenter.org>