PARTNERING TO SAFEGUARD K-12 ORGANIZATIONS FROM CYBERSECURITY THREATS ONLINE TOOLKIT

As of 24 Jan 2023

K-12 organizations are under continued threat from malicious cyber actors, and real-world incidents have demonstrated potentially significant impacts on students, school personnel, and communities. Cybersecurity incidents can result in significant impacts to a school or district's ability to carry out its educational mission and protect sensitive school, student and personnel data. To help schools address these cybersecurity risks, CISA developed a report with recommendations and cybersecurity guidelines for leaders in the K-12 community. The report and this corresponding toolkit are designed to help K-12 schools and school districts most effectively reduce their cybersecurity risks.

In this toolkit, you will find three recommendations along with key actions and related resources to help you build, operate, and maintain resilient cybersecurity programs at your school or district. The toolkit also shares additional free cybersecurity trainings and resources available for the K-12 community.

This toolkit is derived from a broader list of tasks called the Cybersecurity Performance Goals (CPG). The work to improve and maintain your cybersecurity posture should be part of a continuous *program*, not merely a *project* with a finish line. As you work through the tasks below, CISA recommends that you review all the CPGs and plan to incorporate them into your ongoing security program. See https://www.cisa.gov/cpg for more information.

CISA encourages schools and districts to also contact their local regional offices for cybersecurity support and resources. CISA's Cyber Security Advisors (CSAs) can provide schools with cyber preparedness, assessments and protective resources, incident coordination and support for cyber threats and/or attacks, and more.

Expand each recommendation below to learn more and find prioritized action steps and aligned resources to implement at your school or district.

RECOMMENDATION 1: INVEST IN MOST IMPACTFUL SECURITY MEASURES AND BUILD TOWARD A MATURE CYBERSECURITY PLAN

Cybersecurity is not one size fits all. Schools and their districts have distinct strengths and weaknesses and a wide range of needs. At the same time, there are relatively simple actions that every K-12 organization can take to significantly reduce their cybersecurity risks.

IMPLEMENT HIGHEST PRIORITY SECURITY CONTROLS:

1. Implement multifactor authentication (MFA) (Cybersecurity performance goal 1.3)

Description:

MFA is a layered approach to securing online accounts and the data they contain. Even if one factor (such as a user password) becomes compromised, unauthorized users will be unable generally to bypass the second authentication requirement, ultimately stopping them from gaining access to the target accounts.

Action:

All K-12 institutions should review CISA's MFA Enhancement Guide, which provides a defined roadmap toward broad MFA adoption. Ensure that all users with elevated privileges, like system administrators, have MFA enabled for all systems.

Additional resources:

- Multifactor Authentication, CISA
- Phishing-Resistant MFA Fact Sheet, CISA

IMPLEMENT MOST IMPACTFUL SECURITY MEASURES

FIRST

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

SECOND

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

THIRD

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

2. *Identify and fix known security flaws, prioritizing those that are being actively used by malicious actors (Cybersecurity Performance Goal 5.1)*

Description:
While there are many security vulnerabilities in widely used technologies, a small number of these are actually used by malicious actors to compromise victim organizations. By prioritizing these known exploited vulnerabilities, K-12 organizations can significantly reduce their likelihood of compromise.

Action:
Prioritize remediation of vulnerabilities listed in CISA's Known Exploited Vulnerabilities (KEV) Catalog, either by signing up for recurring updates when new vulnerabilities are added or by using a third-party service that automatically identifies the presence of vulnerabilities on the KEV catalog, including but not limited to Palo Alto Networks Cortex, Tenable Nessus, Runecast, Qualys VMDR, Wiz, Rapid7 InsightVM, and Rapid7 Nexpose.

Additional resources:

Known Exploited Vulnerabilities Catalog | CISA

3. *Perform and test backups (Cybersecurity Performance Goal 7.3)*

Description:
Implementing, maintaining, and testing backups of critical data is an essential step to reducing impacts from ransomware and other damaging attacks.

Action:
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 and Google Backup & Sync. 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.

Additional resources:

Data Backup Options

4. *Develop and exercise a cyber incident response plan (Cybersecurity Performance Goal 7.2)*

Description:
Every K-12 organization should have an Incident Response Plan that spells out what the organization needs to do before, during, and after an actual or potential security incident. It will include roles and responsibilities for all major activities, and an address book for use should the network be down during an incident. It should be approved by the senior official in the organization and reviewed quarterly, and after every security incident or "near miss".

Action:
Develop and regularly exercise a written Incident Response Plan, leveraging CISA's Incident Response Plan Basics two-pager with advice on what to do before, during and after an incident. Additional helpful resources include the K12 SIX Essential Cyber Incident Response Runbook and the State Cybersecurity Best Practices Incident Response Plan.

Additional resources:

- Incident Response Plan (IRP) Basics
- The Essentials — K12 SIX

IMPLEMENT ADDITIONAL HIGH PRIORITY SECURITY CONTROLS:

1. Minimize exposure to common attacks (Cybersecurity Performance Goals 2.1 and 5.4)

Description: Malicious cyber actors continuously scan organizations to identify vulnerabilities and execute damaging intrusions. Every K-12 organization should ensure that their Internet-connected assets are up-to-date and free from exploitable conditions.

Actions: Enroll in CISA's free Vulnerability Scanning service and quickly address vulnerabilities identified in recurring reports. Take steps outlined by CISA here to reduce the likelihood that a malicious actor can identify the organization's assets when scanning the internet for potential victims.

Additional resources:

- Cyber Hygiene Services | CISA
- Stuff Off Search | CISA

2. Create a training and awareness campaign at all levels (Cybersecurity Performance Goal 4.3)

Description: All personnel at every K-12 organization should be formally trained to understand the organization's commitment to security, what tasks they need to perform (like enabling MFA, updating their software and avoiding clicking on suspicious links that could be phishing attacks), and how to escalate suspicious activity.

Action: *Review your employee handbook to ensure it has a section on cybersecurity with information on acceptable use of technology, policies, and escalation procedures. Send periodic reminders for staff to review the handbook's security section via email and staff meetings.*

Additional resources:

- Cybersecurity Awareness training (amazon.com)
- Empowering Educators to Teach Cyber | Cyber.org
- Security Awareness Training | SANS Security Awareness

3. Prioritize further near-term investments in alignment with the full list of CISA's Cross-Sectors Cybersecurity Performance Goals (CPGs)

Description: CPGs are a prioritized subset of information technology (IT) and operational technology (OT) cybersecurity practices that all critical infrastructure owners and operators, including K-12 schools, can implement to meaningfully reduce the likelihood and impact of known risks and adversary techniques. They are intended to help establish a common set of fundamental cybersecurity practices that will help schools of all sizes kickstart their cybersecurity efforts.

Action: Review the CPG web site and worksheet, prioritizing goals that the listed as highest impact first. As you develop your monthly, quarterly, and annual roadmaps, include additional Cybersecurity Performance Goals to improve your security posture.

Additional resources:

- Cross-Sector Cybersecurity Performance Goals (CPG)
- CPGs Checklist

4. Over the long-term, develop a unique cybersecurity plan that leverages the NIST Cybersecurity Framework (CSF)

Description:
The CSF is a robust framework for building and maintaining a comprehensive information security program. Governments and enterprises use it to ensure they have covered all the key elements of a mature program.

Action:
Organizations should review the CSF as they complete the tasks here, and in the CPGs. K–12 entities should participate in the free Nationwide Cybersecurity Review (NCSR)22, which provides metrics that identify gaps and track progress, as well as access to incident reporting and cybersecurity resources.

Additional resources:

NIST Cybersecurity Framework, especially the Getting Started page

RECOMMENDATION 2: RECOGNIZE AND ACTIVELY ADDRESS RESOURCE CONSTRAINTS

Most school districts are doing a lot with a little and resource shortfalls can be a major constraint to implementing effective cybersecurity programs. K-12 organizations should take the following steps to recognize and actively address resource constraints:

1. Work with the state planning committee to leverage the State and Local Cybersecurity Grant Program (SLCGP)

Description:
The SLCGP provides $1 billion over 4 years for a first-of-its-kind grant program specifically for state, local, and territorial (SLT) governments funding to support efforts addressing cyber risk to their information systems. The two major first year requirements for this program include the establishment of a Statewide Cybersecurity Planning Committee and the development, by this committee, of a Statewide Cybersecurity Plan. Public Education is a required member of the Planning Committee, therefore ensuring the cybersecurity needs of educational institutions are accounted for. While the funding is granted directly to the State Administrative Agency, publicly funded K-12 schools are eligible to receive sub-award money.

Action:
Review the resources below to determine your school's eligibility and consider applying to the program.

Additional resources:

- FY22 State and Local Cybersecurity Grant Program Fact Sheet, CISA
- State and Local Cybersecurity Grant Program Frequently Asked Questions, CISA
- Homeland Security Grant Program, FEMA
- Homeland Security Grant Program (HSGP) Application Process, FEMA

2. Utilize free or low-cost services to make near-term improvements when resources are scarce

Description:
As part of our continuing mission to reduce cybersecurity risk across U.S. critical infrastructure partners and state, local,

tribal, and territorial governments, CISA has compiled a list of free cybersecurity tools and services to help organizations further advance their security capabilities. This living repository includes cybersecurity services provided by CISA, widely used open-source tools, and free tools and services offered by private and public sector organizations across the cybersecurity community. CISA will implement a process for organizations to submit additional free tools and services for inclusion on this list in the future.

Action:
Evaluate your security program's need for services and tools to determine if any in this catalog are a fit for your needs.

Additional resources:

Free Cybersecurity Services and Tools, CISA

3. Ask more of technology providers

Description:
K–12 organizations should expect the technology used for core educational functions like learning management and student administrative systems to have strong security controls enabled by default for no additional charge.

Action:
During the technology procurement and renewal process, ensure that vendors do not charge more for security features like MFA and logs. Be especially aware of the "SSO tax", the practice of changing customers more to connect a service (like a financial or time keeping system) to the organization's Single Sign On (SSO) portal. Further, as you deploy products be sure to review the product's "hardening guide". A hardening guide is a set of steps to make the product less dangerous. As you become aware of upcharges for security features, or unsafe defaults, start a dialog with other schools and ISAC members to assess a strategy for working together with the vendor to remediate. CISA is ready to serve as an advocate for the K-12 community in advancing technology products that are fit for purpose to support our nation's education system. Where a K-12 organization identifies as technology that is not meeting expectations for security built-in, contact your regional cybersecurity advisor to begin a conversation on how we can help.

***Additional resources*:**

Cyber Security Advisors, CISA

4. Minimize the burden of on-prem security

Description:
Many K–12 organizations operate their own IT systems, known as "on premises" systems. 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

Action:
K–12 organizations should urgently consider migrating on-premises IT services to the cloud. While it is not possible to categorically state that "the cloud is more secure," migration to the cloud will be a more secure and resilient option for many K–12 organizations. Consider first cloud versions of your user identity system, and your mail system. Talk to your CISA regional representative for guidance on secure cloud migration.

Additional resources:

- Google Workspace | Business Apps & Collaboration Tools
- Azure Active Directory | Microsoft Azure
- Microsoft 365 - Subscription for Office Apps | Microsoft 365

RECOMMENDATION 3: FOCUS ON COLLABORATION AND INFORMATION SHARING

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

Description:
By focusing on collaboration and information sharing, K-12 organizations can stay aware of critical alerts on current threads and vulnerabilities.

Action:
Join cybersecurity collaboration groups, such as MS-ISAC and K12 SIX. MS-ISAC membership includes reporting as well as data and information sharing. In addition, MS-ISAC K-12 community members receive critical alerts on current threats, risks, and vulnerabilities; free cyber tools, resources, and services; and 24/7 access to assistance that includes threat incident analysis, mitigation, and remediation.

- Join MS-ISAC – Free for U.S. State, Local, Tribal & Territorial Government Entities, Center for Internet Security (CIS)
- K12 SIX Member Benefits, K12 SIX

Action:
Work with other information-sharing organizations, such as fusion centers, state school safety centers, other state and regional agencies, and associations.

State Information Sharing Tool, SchoolSafety.gov

Action:
Build a strong and enduring relationship with CISA and FBI regional cybersecurity personnel. Report every cyber incident to CISA, every time.

- Regional Offices where you can get connected with our Cybersecurity Advisors, CISA
- Report to CISA, CISA
- Internet Crime Complaint Center (IC3), FBI

ADDITIONAL RESOURCES AND TRAINING FOR K-12 STUDENTS AND EDUCATORS

Federal Virtual Training Environment (FedVTE) Public Courses: This training environment offers more than 800 hours of free online, on-demand cybersecurity training for state, local, tribal, and territorial government personnel and veterans, including K-12 schools.

Foundations of Cybersecurity Management, National Initiative for Cybersecurity Careers and Studies (NICCS): This free online, instructor-led course teaches you how to apply the principles of cybersecurity management.

Fundamentals of Cyber Risk Management, NICCS: This free online, self-paced course focuses on key concepts, issues, and considerations for managing cyber risk.

Don't wake up to a Ransomware Attack, NICCS: This free online, self-paced course provides essential knowledge and reviews real-life examples of cyber attacks to help you and your organization to prevent, mitigate, and respond to the ever-evolving threat of ransomware.

SchoolSafety.gov Cybersecurity Topic Page: This webpage hosts federal government resources, guidance, and tools on cybersecurity for K-12 schools.

Cybersecurity Training and Exercises, CISA: This webpage lists CISA trainings available to non-federal cybersecurity professionals and the public, including K-12 schools.

NICCS Education and Training Catalog: This catalog is a central location to help cybersecurity professionals of all skill levels find cybersecurity-related courses online and in person across the nation.

CETAP Cyber Safety Videos, Cyber.org and CISA Counselors: This video series provides tips for staying safe online. Topics include: the Internet of Things; Social Media Safety; Ransomware; Phishing; Making Strong Passwords; Online Gaming Safety; and Video Call Safety.

Cybersecurity Considerations for K-12 Schools and School Districts, REMS-TA Center: This training course is designed to help K-12 schools and districts understand cybersecurity considerations needed to inform school emergency operations plans and safety, security, emergency management, and preparedness programs.

Carnegie Mellon University, This free computer security education program for students and teachers provides original content built on a capture-the-flag framework created by security and privacy experts at Carnegie Mellon University.

For additional information, download the Partnering to Safeguard K-12 Organizations from Cybersecurity Threats report.

Note: *This toolkit is not comprehensive. CISA applies neutral principles and criteria to add items and maintains sole and unreviewable discretion over the determination of items included. CISA does not attest to the suitability or effectiveness of these services and tools for any particular use case. CISA does not endorse any commercial product or service. Any reference to specific commercial products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply their endorsement, recommendation, or favoring by CISA.*