Cybersecurity Resource Guide

Planning Resources

- Computer Security Resource Center (National Institute of Standards and Technology [NIST], U.S. Department of Commerce). This NIST Website provides cybersecurity- and information security-related projects, publications, news and events.
  Audience: IT personnel

- Critical Infrastructure Cyber Community (C^3) Voluntary Program (U.S. Department of Homeland Security [DHS]). To help organizations that want to use the *Framework for Improving Critical Infrastructure Cybersecurity* to strengthen their IT networks and systems, DHS launched the C^3 program. The program connects organizations to federal departments and agencies and the private sector with expertise in managing cyber risks and provides cyber-related resources.
  Audience: IT teams

- Cybersecurity Considerations for K-12 Schools and School Districts Fact Sheet (Office of Save and Healthy Students [OSHS] & REMS TA Center). In this publication, a brief introduction to common cyber threats facing schools is presented. Specific steps to take before, during, and after a cybersecurity incident are identified.
  Audience: IT teams, planning teams, administrators

- Cybersecurity Framework Web Page (NIST). The Cybersecurity Framework includes standards, guidelines, and best practices to address cyber threats, and includes steps to Identify, Protect, Detect, Respond, and Recover. Testimonials on the use of the Framework are included in a Perspectives tab.
  Audience: IT teams

- Enhanced Cybersecurity Services (DHS). This program helps protect computer systems against unauthorized access, exploitation, and data exfiltration through email filtering, the blocking of specified malicious domain names, and passive detection of threats.
  Audience: IT teams, administrators

- Framework for Improving Critical Infrastructure Cybersecurity (NIST). The voluntary Framework was developed as a collaborative effort among government agencies and departments, academia, and the private sector to help organizations manage their cybersecurity risks.
  Audience: IT personnel

- Integrating Cybersecurity with Emergency Operations Plans (EOPs) for K-12 Schools Webinar (OSHS, U.S. Department of Homeland Security [DHS] & REMS TA Center). In this archived Webinar, presenters provided an overview of the landscape of cyber threats facing K-12 schools. Also shared were resources, programs, and tools to help schools maintain secure networks and prevent cyber attacks.
  Audience: IT teams, planning teams, administrators

- OET Website (U.S. Department of Education). On this Website, viewers will find initiatives, resources, and publications related to national educational technology strategies and policies.
  - Building Technology Infrastructure for Learning Guide. This publication contains cybersecurity information in Section 3: *Getting High-Speed Internet Throughout Schools*.

  Audience: IT teams, planning teams, administrators

- SITE ASSESS Planning Tool (OSHS & REMS TA Center). SITE ASSESS is a secure and comprehensive mobile application that allows school district and school (public and nonpublic) personnel to walk around a school building and grounds and examine their security, safety, accessibility, and emergency preparedness. Included within the section on Computers and Network Systems are tasks that examine cybersecurity.
  Audience: Planning teams, administrators

Data Security

- Protecting Student Privacy Website (PTAC and Family Policy Compliance Office). This Website contains information and resources for education stakeholders on data privacy, confidentiality, and security practices related to student-level data systems and other uses of student data.
  - Data Security and Management Training: Best Practice Considerations. This best practices guide describes strategies schools and school districts can adopt to ensure that staff members are adequately aware of, and trained in, critical data security principles such as breach detection and escalation, forms of data breaches, and data backup and disaster recovery.
  - Data Security Checklist. This checklist is designed to assist stakeholder organizations with developing and maintaining a successful data security program by listing essential components that should be considered when building such a program, with a focus on solutions and procedures relevant for supporting data security operations of educational agencies.
  - Data Security: Top Threats to Data Protection. This publication outlines critical cyber threats to educational data and information systems, and includes suggestions for mitigating the threat.
  - Data Breach Response Training Kit. This downloadable training package contains a facilitator's guide, PowerPoint presentation, and handouts on a password data breach

scenario. This interactive exercise is intended to assist schools and school districts with internal data security training, including examining processes, procedures, and skills needed to respond to a data breach.

- W2 Phishing Scam Now Targeting Schools. This Internal Revenue Service (IRS) guidance highlights ongoing phishing attacks against K-12 schools and school districts. These attacks are targeting human resources and critical business functions within organizations to access the Personally Identifiable Information from the W-2 forms of employees and, in some cases, are extracting fraudulent payments from their victims. This document contains a summary of the attacks, tactics of the attackers, potential ramifications, and links to the official IRS guidance.

Audience: IT teams, planning teams, administrators

- CyberAdvisory: New Type of Cyber Extortion/Threat Memo (Office of Federal Student Aid, ED). This memo details how criminals are attempting to extort money from educational entities—including schools and school districts—by threatening to release sensitive data from student records. The memo describes how to protect IT network and systems and what to do if an educational entity is affected by this type of threat.
  Audience: IT teams, planning teams, administrators

Education

- Integrating Cybersecurity Into the Classroom (National Initiative for Cybersecurity Careers and Studies). This program offers professional development opportunities to middle school teachers and high school teachers so that they can integrate cyber components into their lessons and projects.
  Audience: Administrators, teachers

- Stop.Think.Connect. Program (DHS). This national public awareness effort increases the understanding of cyber threats and empowers the American public to be safer and more secure online. The Stop.Think.Connect. Toolkit contains materials for K-8 students, 9-12 students, and students at institutions of higher education, as well as parents and K-12 educators.
  Audience: Planning teams, administrators

- Staying Safe Online at School Web Page (National Cyber Security Alliance). On this Web page, information is provided to administrators on how to raise awareness about cyber threats, teach people to Stop.Think.Connect., and evaluate and update cybersecurity plans.
  Audience: Administrators