

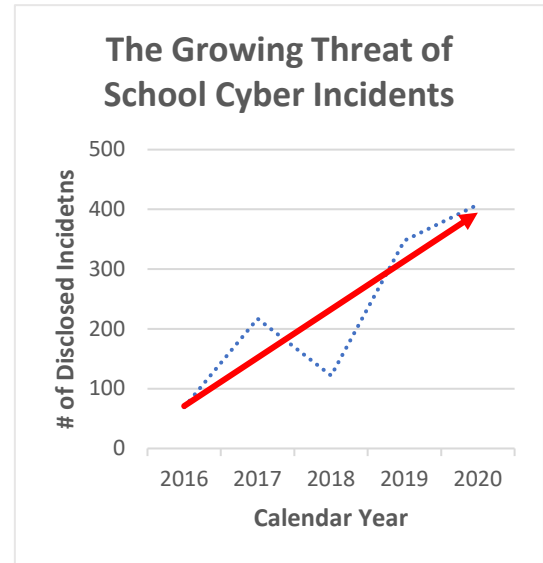


K12 SIX Essential Cybersecurity Protections: 2021-2022 School Year

Despite billions of U.S. taxpayer dollars invested annually in technology for teaching, learning, and school operations—and despite evidence of the increasing frequency and severity of K12 cybersecurity incidents—there does not yet exist a meaningful consensus about what cybersecurity protection a student, parent, or teacher can expect from their schools.

While there is no shortage of best practice guidance available from government and private sources, that guidance often presumes greater IT capacity and resourcing than most school districts can afford. Moreover, general guidance is not well-suited to the specialized software applications and cultural realities of technology implementation in K12 settings, designed as they are to serve the diverse and specialized needs of large numbers of children and youth.

The K12 Security Information Exchange ([K12 SIX](#)) launched in late 2020 with the sole aim of helping school districts and other K12 organizations—including charter schools, private schools, and state and regional education agencies—to better defend themselves from emerging cybersecurity threats, such as ransomware and phishing attacks. The non-profit K12 SIX operates as an enhanced information sharing and analysis center (ISAC), fostering collaboration amongst its members to achieve collective defense against cyber threats.



Source: "The State of K-12 Cybersecurity: 2020 Year in Review." Available online at: <https://k12cybersecure.com/year-in-review/>

With the explicit aim to address the security capability and expectations "guidance gap" in school district cybersecurity practices, K12 SIX is pleased to release the first in a series of K12-specific cybersecurity risk management products: "K12 SIX Essential Cybersecurity Protections: 2021-2022 School Year."













This document defines a short list of actionable cybersecurity controls that all school districts should prioritize for implementation this year.

Developed by K12 IT practitioners, for K12 IT practitioners—and aligned to cybersecurity risk management best practices—the K12 SIX-recommended protective measures are designed to defend against the most common cyber threats facing school districts, including those recently



identified by the Federal Bureau of Investigation (FBI) and the Cybersecurity & Infrastructure Security Agency (CISA).

The *K12 SIX Essential Cybersecurity Protections* consist of a dozen cybersecurity controls—grouped into four categories—that every school district should strive to implement:

Recommended Protective Measure	Description
1.0 Sanitize Network Traffic to/from the Internet	
 1.1 Filter out malware	Block access to known malicious websites
 1.2 Campaign against email scams	Reduce the odds that email-based social engineering attacks succeed
 1.3 Block malicious documents	Block access to malicious office suite documents, commonly responsible for ransomware
 1.4 Limit exposed services	Limit internet exposure of services like remote desktop protocol (RDP)
2.0 Safeguard Student, Teacher, and Staff Devices	
 2.1 Restrict administrative access	Keep devices protected and in compliance with security policies
 2.2 Apply endpoint protection	Ensure devices used for school remain safe whether used on or off premises
3.0 Protect the Identities of Students, Teachers, and Staff	
 3.1 Protect user logins	Implement multi-factor authentication (MFA) to safeguard against compromised passwords
 3.2 Improve password management	Prevent password compromise, sharing, and re-use—commonly responsible for data breaches
 3.3 Stop online class invasions	Ensure online classes can only be attended by authorized teachers and students
4.0 Perform Regular Maintenance	
 4.1 Install security updates	Protect against known vulnerabilities through timely patching of IT systems, computers, and equipment
 4.2 Backup critical systems	Build resilience against destructive attacks like ransomware through offline, immutable backups
 4.3 Manage sensitive data	Ensure sensitive data is protected, archived, and deleted when no longer needed



School districts that implement these protective measures will be less likely to experience significant cyber incidents involving the breach of student data, interruptions in teaching and learning, and the theft of funds. Careful consideration has been made to emphasize protective measures that can be reasonably and cost-effectively implemented in most typical K12 settings. Nonetheless, their implementation should not be construed as a guarantee of the cybersecurity of school district-managed IT systems and data, nor should the implementation of these protective measures be considered a substitute for instituting a comprehensive cybersecurity risk management program.

Forthcoming K12 SIX products in this series will provide:

- ‘Standards of Practice’ for implementing each of the K12 SIX recommended protective measures
- K12-specific implementation advice for each K12 SIX recommended protective measure
- A free, online cybersecurity self-assessment tool for school district IT leaders aligned to the K12 SIX Standards of Practice
- Communication templates that school district IT leaders can customize to help convey cybersecurity risk management recommendations to their school board, superintendent, and/or other senior leadership

Questions or comments about this product series—including about how your school district can join the non-profit K12 SIX to enhance your district’s cybersecurity risk management practices—can be directed to info@k12six.org or visit <https://www.k12six.org>.