The Essential Cybersecurity Service You've Never Heard Of

No-cost membership in the MS-ISAC can help protect your school from the growing cybersecurity threat.

Josh Moulin
Senior VP of Operations and Security Services
Center for Internet Security (CIS)

THE CYBERSECURITY THREAT TO K-12 educational institutions has been consistently growing since 2018. Unfortunately, for many schools, efforts to protect against cyber-attacks have not seen similar growth. K-12 public schools became the number one target for ransomware attacks across all public sectors in 2020. Meanwhile, less than a quarter of school districts have anyone dedicated to network security, according to the latest **CoSN leadership report**. And even institutions with dedicated network security staff may struggle with a lack of funding to dedicate to cybersecurity measures. This poses a challenge for schools that cannot build cybersecurity defenses that match the sophistication of the malicious actors intent on attacking their data-rich networks.

Fortunately, cybersecurity help is available, and at no cost. Recognizing that schools, along with other state, local, tribal and territorial government agencies, rarely have the resources they need for cybersecurity, the **Center for Internet Security**, an international nonprofit, offers essential cybersecurity services through the **Multi-State Information Sharing & Analysis Center (MS-ISAC)**.

Schools and districts can join the MS-ISAC for free, and by doing so they gain access to a number of no-cost services that will assist those school systems in achieving their cybersecurity goals. While there are numerous benefits, like advisories, members-only webcasts and cybersecurity reviews, here are three of the most essential services worth noting:

- ***24/7 support from our team of experts running the Security Operations Center.*** You can call at any time and speak to our world-class cybersecurity experts about any network challenges or questions.
- ***Incident response services through our Cybersecurity Incident Response Team (CIRT).*** If you believe your district has been a victim of a cyber-attack, this team is prepared to guide you during a response as well as afterward, as you uncover the extent of the problems and close up the vulnerabilities.
- ***Malicious Domain Blocking and Reporting (MDBR).*** This DNS security service, powered by technology from **Akamai**, helps protect your organization from any type of web query or e-mail link your users might click. MDBR checks the given domain to make sure it is not on the list of known malicious domains. Akamai's built-in machine learning not only compares the query to known bad domains but also considers whether there are other aspects to the activity that should raise red flags. Is this domain similar to other known bad domains? How new is this domain? Did somebody buy it within the last 24 hours? If there is a suspicion that the domain is malicious, the request will be blocked and a window will pop up telling the user that the domain has been flagged as potentially malicious. We stop millions of requests every day through the service, and there's no delay in user performance. MDBR has been highly effective in stopping phishing and other malware schemes that get through the firewall or other protective measures.

Preventing Security Emergencies

While a major goal of the MS-ISAC's program is to help schools deal with security emergencies as they are happening, another objective is to partner with them to prevent those emergencies in the first place. We recommend schools consider several actions to help prevent cybersecurity incidents.

An easy first step is to become a member of the MS-ISAC. That is the best way to take advantage of the free products and services we offer, like MDBR, which will provide immediate protection in as little as 15 minutes.

Next, it is important to gain district leadership support for creating a comprehensive cybersecurity and risk management program. Cybersecurity belongs alongside weather events and other natural disasters as part of a holistic risk profile for your schools. The customizable materials we produce and make available through the MS-

About CIS Critical Security Controls

The **CIS Critical Security Controls** are a series of cybersecurity best practices, a prioritized set of actions for protecting your district and data from cyber-attack vectors, which you implement based on your school system's level of risk tolerance. In many cases, CIS offers no-cost open source tools to aid in implementing the Controls. **Learn more about MS-ISAC on the CIS website.**

ISAC can support you in those conversations.

Similarly, take advantage of templates and other pre-made resources we offer that will amplify communications about your cybersecurity efforts and broadcast your security concerns. We want to partner with you to help tell your cybersecurity story.

Also, consider implementing the CIS Critical Security Controls and a CIS SecureSuite membership, both of which are free of charge for MS-ISAC members. The Controls are a proven way to reduce risk and increase cybersecurity maturity within an organization. In fact, some states have begun mandating use of the CIS Controls as a cybersecurity framework. SecureSuite (also free to public schools) is software designed to automate implementation of some of the Controls.

Finally, it is important to review the rapid changes and new tools introduced during the pandemic. Any kind of security assessment should incorporate lessons learned from the broader K-12 community into your school's cybersecurity program. You don't have to do all of this alone. Currently, some 2,800 K-12 districts have signed up for the MS-ISAC service, and we have started a K-12 workgroup to help promote cybersecurity information sharing and cooperation among schools. Still, more than 100,000 schools have yet to join the MS-ISAC and benefit from our no-cost services. If your school has not yet joined, we are standing by, ready to help.

Recognized globally *for his expertise in cybersecurity, Josh Moulin is the Senior Vice President of Operations & Security Services at the Center for Internet Security (CIS) and has worked in cybersecurity since 2004. Prior to joining CIS, Moulin was an Executive Partner at Gartner and advised Federal Government and defense executives, a CIO and CISO within the U.S. nuclear weapons complex, and a commander of an FBI cybercrimes taskforce. He holds a master's degree in Information Security & Assurance and over a dozen certifications in digital forensics and cybersecurity.*