AI FOR GOOD

LEVERAGING AI TOOLS IN CYBERSECURITY

The Multi-State Information Sharing & Analysis Center (MS-ISAC) reported that 82% of schools and districts have experienced some kind of "cyber incident. Cyber incidents disrupt instruction, expose student data, and strain already limited IT resources and one in three districts reports lacking dedicated cybersecurity staff, leaving schools increasingly vulnerable as attacks grow in frequency and sophistication. Artificial intelligence (AI) tools can help districts augment their cybersecurity programs by improving planning, strengthening prevention and detection, supporting staff training, and prioritizing limited resources more effectively. When used thoughtfully, AI does not replace human judgment or governance; it enhances the capacity of existing teams to operate more strategically and proactively.

AI is no longer a futuristic concept for cybersecurity; it has been evolving for years through machine learning and automation. Today, leveraging AI is a necessary step; avoiding it is not an option, as adversaries are already using AI to exploit vulnerabilities. This document outlines practical ways school districts can leverage AI tools to build, refine, and continuously improve their cybersecurity posture, with a particular focus on how smaller districts can benefit.

Using AI to Strengthen Core Cybersecurity Functions

1. Cybersecurity Planning and Documentation

AI-powered chatbots can be used to accelerate cybersecurity planning by helping staff fill in templates for required documents such as:

- Incident Response Plans
- Disaster Recovery and Business Continuity Plans
- Acceptable Use Policies
- Data Privacy and Security Procedures

By prompting AI with district-specific details (size, systems used, student population, regulatory environment), districts can quickly generate draft plans that staff can review, refine, and approve. This reduces the barrier to maintaining up-to-date documentation and helps ensure consistency across plans.

Try these ideas in a chatbot tool:
• Upload CoSN's Disaster Recovery Plan template (https://www.cosn.org/tools-and-resources/resource/disaster-recovery-plan-template/?ssoSuccess=1769189689N8AR), and ask the

chatbot to help you fill it out for one of your systems.
• Upload a sanitized copy of your district's cybersecurity insurance policy and ask the chatbot to create a one page do's and don'ts list from that policy. This is a fast way to create a checklist to ensure actions taken in an incident don't void your policy.
• Upload one or two metrics from your district security program and ask the chatbot to create infographics for a report.

2. Tabletop Exercises and Incident Readiness

RAI can significantly enhance tabletop exercises by:

• Generating new and realistic incident scenarios (e.g., ransomware, phishing, data breach, system outage)
• Adapting scenarios based on district size, technology stack, and threat trends
• Acting as a facilitator by prompting discussion questions and next steps

Using AI in this way allows districts to run tabletop exercises more frequently and with less preparation time, improving readiness without adding staff burden. Over time, AI-generated scenarios can help identify gaps in procedures, communication flows, and decision-making authority.

Try these ideas in a chatbot tool:
• Upload a sanitized version of your incident response plan and ask for help creating a tabletop incident response exercise that will allow you and your team to test the plan. Request prompts for facilitating the tabletop exercise.
• Ask the chatbot to create a tabletop exercise using a specific scenario such as, "Create a tabletop exercise scenario for a K-12 district where a staff member clicked a phishing link and attacker access has spread to multiple accounts. Include a timeline of discovery, decision points about notifying parents and staff, and questions about containment vs. continuity of operations."

3. Cyber Playbooks and Decision Support

Cybersecurity playbooks can be uploaded into AI tools, allowing staff to ask questions such as:

• "What steps should we take first in this type of incident?"
• "Who should be notified based on our procedures?"
• "What compliance obligations apply in this scenario?"

This transforms static documents into interactive resources, giving IT staff and administrators quick access to context-aware guidance during both planning and live incidents.

Don't have cybersecurity playbooks yet? Load a scenario into your AI chatbot and ask it to create a cybersecurity playbook for responding to this scenario. Remember to proof read, test and edit the playbook carefully before you add it to your incident response plan.

Try this idea in your chatbot tool:
Ask the chatbot to create a cybersecurity incident response playbook for the scenario where a

staff member clicked a phishing link and their credentials were compromised.

4. Improving Compliance and Privacy Alignment

AI tools can assist districts in improving compliance with national and state data privacy laws by:

- Identifying gaps or inconsistencies in documentation
- Mapping current policies and practices against regulatory requirements
- Summarizing legal or regulatory language into actionable steps

When compliance reviews are completed, AI can help analyze findings and build a prioritized action plan that aligns remediation efforts with the district's highest risks and available resources.

Try this idea in your chatbot tool:
Upload a sanitized version of your compliance review removing all district identifiable and confidential information into your AI chatbot. It is recommended you utilize a licensed AI chatbot where your data is not used to train public models (avoid doing this in the public AI space). Ask the chatbot to summarize the findings and build a prioritized action plan that prioritizes actions based first on level of risk and then on the amount of resources necessary to complete the remediation task.

5. Using Audit Results to Drive Priorities

Audit reports often contain valuable insights but can be time-consuming to translate into action. AI tools can:

- Summarize audit findings
- Group issues by risk level or theme
- Recommend phased remediation plans
- Generate task lists tied to timelines and ownership

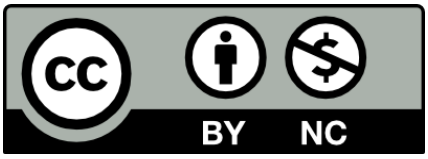
This approach helps leadership focus on what matters most and ensures that audit findings lead to measurable improvements rather than stalled reports.

Try this idea in your chatbot tool:
Upload your sanitized audit report into your licensed AI environment (never do this in the public AI space) and ask the chatbot to summarize the findings by theme and recommend a phased remediation plan.

AI tools offer school districts opportunities to improve planning, readiness, compliance, and efficiency, especially for districts with limited staffing. By integrating AI thoughtfully, tuning systems, applying prompt engineering, and monitoring outputs, districts can use AI as a powerful ally in defending students, staff, and systems.

Cautionary Notes and Best Practices

• Avoid entering sensitive or confidential data into AI systems without strong protections. Do not use publicly available AI spaces for sensitive content, make sure you are using a licensed and protected access that prevents your data from being used to train the vendor's large language model.
• Double check everything and validate the outputs of all AI queries. Proof read your content.
• Treat AI-generated content as a draft; always validate before taking action.
• Monitor AI behavior and outputs regularly to detect errors or misuse.
• Understand what AI might block or restrict.
• Use AI as a support tool; critical decisions should remain with trained personnel.
• When in doubt, assess your utilization of AI against the NIST AI Risk Management Framework (https://www.nist.gov/itl/ai-risk-management-framework)



CoSN
Leading Education Innovation