LEADING EDUCATION INNOVATION

CONDUCTING A CYBERSECURITY RISK ASSESSMENT

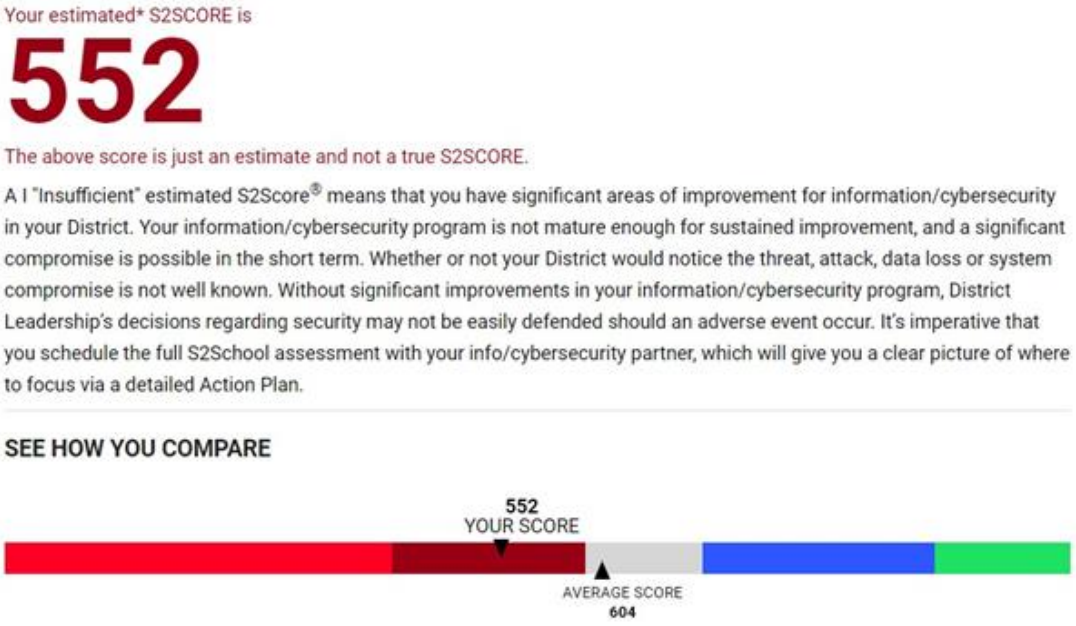
What is a Cybersecurity Risk Assessment? Why should I do one?

Risk management is critical for districts to successfully implement and maintain a secure teaching and learning environment. Risk assessments identify, quantify, and prioritize risks against criteria established by the district for risk tolerance and objectives. Assessment results guide and determine appropriate district action and priorities for managing information security risks and for implementing controls needed to protect information assets.

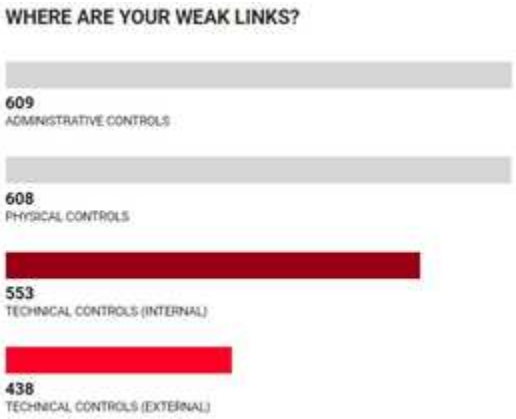
What is the CoSN Risk Assessment Tool?

CoSN partnered with Security Studio (S2) to develop a free, entry level risk assessment specifically designed for K12 schools. This risk assessment is 80 questions long and covers the following areas: background information, administrative controls, physical controls, and technical controls. All questions about security controls are limited to yes/no responses.

Once the assessment is completed, it instantly provides an estimated CoSN Cybersecurity Risk Assessment Powered by S2 risk score with an explanation of where the district is in their security journey and benchmarks the result against similar districts nationally. The maximum score possible on the assessment is 850. Here is an example:



The score provided by the CoSN Cybersecurity Risk Assessment Powered by S2 is an **estimated score** and is not validated or confirmed by CoSN. In addition to the total score, the results also provide a breakdown by control area. For example:



Accessing the Risk Assessment

The CoSN Risk Assessment powered by S2 is located at: https://securitystudio.com/CoSN/
When you get to the risk assessment, you will have to complete three questions to start the assessment. You must accept the agreements and terms and to share information with CoSN. Please be aware that the information that is shared with CoSN is aggregate data, it is not individually identified data for your district.

You are not required to provide your contact information to access the survey. You may opt to receive a follow-up from SecurityStudio regarding your score. Under the terms of CoSN's agreement with SecurityStudio, agreeing to receive a follow-up from Security Studio means that you will receive **one outreach call** from that organization. They will not contact you multiple times.

Perfection is not the Goal

You should not have a perfect score of 850. If you score a perfect score on this assessment, it is likely that you are overstating your cybersecurity capabilities. The assessment limits you to yes/no responses so if you only have part of a response covered then make sure you score the response to that question as "No".

Leveraging Risk Assessment Results

This free risk assessment is an entry point for conducting risk assessment and improving the security posture of an organization through risk assessment. There are several effective steps that you can take to use the information obtained in the risk assessment.

1. Identify security gaps and make plans to close the gaps. Select a realistic number of items to work on (3-5) and document the steps that will be taken to reduce the risk in each area.
2. Communicate district security posture to district leadership - the risk assessment provides a quick and easy visual summary of existing security risks. Share the risk assessment and the improvement plan with district leadership and leverage the risk assessment results to discuss with leaders their level of risk tolerance. The risk assessment can be a tool to support budget requests. Remember to involve district leadership in prioritizing and approving critical decisions and changes, and obtain sign off on the plan.
3. Gamify the results. Retake the assessment as improvement efforts are completed and document and celebrate changes in the score.

Using this entry level risk assessment is a starting point. In cybersecurity the work is never complete, instead, the emphasis is on continuous improvement and ongoing risk reduction. This tool provides a starting point for using risk assessment. As the district's risk assessment process matures, look for opportunities to move to a more advanced or in-depth risk assessment tool and to work with an outside risk assessment professional who will identify additional opportunities for risk reduction.

CoSN RESOURCES

CoSN Risk Assessment powered by S2- https://securitystudio.com/CoSN/

About CoSN:

CoSN, the national association of school system technology leaders, believes that technology is an essential component of learning today, and is deeply committed to the use and distribution of technology in school systems. However, all technologies must be properly assessed for design and appropriateness in the modern classroom. Educators and companies alike must recognize and uphold their responsibilities to protect the privacy of student data.

Working together, educators and the private sector serve millions of students by providing them with the rich digital learning experiences and access needed to succeed in college, work and life. That partnership is critical to ensuring that students will have the tools necessary for success in the 21st century.

Consortium for School Networking 1325 G St, NW, Suite 420, Washington, DC 20005