LEADING EDUCATION INNOVATION

Annual Report
CoSN Risk Assessment

Background

In 2020, CoSN partnered with Security Studio (S2) to develop a free, entry-level risk assessment designed explicitly for K12 schools and is available to all schools. This risk assessment is 80 questions long and covers the following areas: background information, administrative controls, physical controls, and technical controls. In addition, all questions about security controls are limited to yes/no responses. This report summarizes the results of schools and districts across the USA who completed the CoSN Risk Assessment powered by S2 between May 2020 and May 2021.

The data that was collected from more than 120 school systems ranged from districts with 16 to 350,000 students. The mean technology team size was 4 FTE. 15 % of responding organizations indicated one or fewer full-time technology staff.

Results

Key areas of concern include:

- Risk Management
- Air Gapped & Validated Backups
- Encryption
- Awareness Training

As is common in K-12 education, most schools and districts rank high in physical controls and lack administrative and technical controls.

Significant Risks

The aggregated results identify several significant risks to schools and districts.

- **Risk Management** Majority of responding schools and districts do not have strong risk management programs. However, a small majority have cybersecurity liability insurance. Please note the risk assessment did not differentiate between full coverage and coverage under an umbrella plan.

- **Human Capacity** 76.8% of responding schools and districts indicate that someone is designated with cybersecurity responsibility; however, over half of those responding don't have a formal cybersecurity program supported by leadership.

• **Employee Training** Employee training is one of the top steps a school or District can take to protect from cybersecurity incidents. Yet, only 44.8% of respondents indicate they have any cybersecurity awareness or training program.

• **Administrative Rights** While over 70% of respondents report their users don't have administrative rights on their machines, this is inconsistent with other K12 reporting sources and may indicate an area where the respondent made an incorrect assumption about the security of their systems. Access to privileged accounts and the accumulation of rights across systems are significant cybersecurity threats.

• **Encryption** During a cybersecurity incident that involves data theft or loss, encryption is considered the gold standard for avoiding having to declare a data breach. However, less than 35% of respondents use data encryption to protect data in transit and at rest.

• **Backups** While the majority of respondents report conducting regular data and system backups, only about half of them test and validate their backups regularly. It is important to note that the risk assessment does not distinguish between air gapped vs. online backups. Given the low rates of encryption at rest reported, it is unlikely that the majority of these respondents are encrypting their backups.

• **Independent Reviews** Upon reviewing the technical controls, the responses seem slightly high based on experience reviewing K12 organizations. However, given that only 28% of respondents have an outside independent party conduct a security review, audits or assessments are performed on an annual basis, these responses may be overestimating the respondent's school or district's capabilities.

Data

Once the assessment is completed, it instantly provides an estimated risk score with an explanation of where the District is in its security journey and benchmarks the result against similar districts nationally.

Among the schools and districts that used the Risk Assessment in 2020-21, the mean score was 636 or Progressing, out of a total possible score of 850. Progressing is defined as:

P "Progressing" estimated S2Score® means that you have done some good things with respect to your District's information/cybersecurity; however, significant gaps/risks still exist. Some of the foundational components of the program are in place, and it's time for the program to mature into a more formal initiative. This is the point in the program where information/cybersecurity efforts and investments need to provide accurate and tangible results. The question, "where should we focus our time and investments?" is important to support facts instead of gut instinct. Start by scheduling the full S2School assessment with your info/cybersecurity partner, which will give you a clear picture of where to focus via a detailed Action Plan. A compromise is still very much possible, but you are more likely to detect it and respond with some effectiveness. If District Leadership is involved with information/cybersecurity, which they probably are, continued improvement will only help them make better risks.

In understanding the data collected from the Risk Assessment, it is essential to recognize the following:
• The data does not reflect or include the role of the responder. Therefore, it is possible that responders

could be overestimating their degree of security based on their role in the organization. For example, education technology professionals may be more likely to assume their firewall and network defenses meet the descriptions in the technical control sections.
• The results below are based on self-reporting and have not been validated through a review of the participant's responses and supporting documentation by an accredited security professional.

Conclusion

The analysis of a years' worth of aggregated risk assessments is consistent with the CoSN Ed Tech Leadership Survey results, which identified a significant concern that "Specific cybersecurity risks are generally underestimated even though cybersecurity and the privacy/security of student data are the top two technology priorities." As a result, schools and districts continue to struggle in crucial prevention areas and would benefit by focusing on achieving three specific steps:

1. consistent implementation of security awareness training for all employees
2. encrypting data in transit and at rest
3. implementing and testing air gapped backups to ensure recoverability of data in a ransomware attack or disaster event.

Beyond these specific steps, schools and districts would benefit from investing time and effort into developing or extending their risk management practices encompassing cybersecurity within their organizations.