How to Build a Cybersecurity Program

Why does my district need a cybersecurity program?

School districts routinely collect, store, and access hundreds of pieces of protected personally identifiable information and educational records for students and staff. The responsibility to secure information and the systems storing that data, ensure resources are available when needed, and protect the privacy of data resides with each individual school district. This triad of responsibilities is often referred to as maintaining confidentiality, integrity, and availability (CIA) of school district systems and data.

Failure to protect student and staff information can result in financial and reputational loss including significant costs for resolving a data breach or cybersecurity attacks, and loss of confidence in the district by the public. Additionally, failure to protect personal information of staff and students may compromise their physical safety and financial well-being now or in the future. Safety, privacy, legal responsibility, and regulatory compliance are all reasons for establishing a cybersecurity program.

What is a cybersecurity program?

A cybersecurity program consists of a thorough and documented approach to cybersecurity and privacy that requires three distinct areas to be addressed: people, processes, and technology. The program requires a sponsor, or champion at the executive level who is accountable for ensuring that the program is provided visibility and support, and a program leader who is responsible for leading the program. Ultimately, a cybersecurity program is designed to build a culture of cybersecurity within the school system.

People

The risk of human error and misuse of information and equipment is ever-present. There are many ways to address the people component of cybersecurity in the program. Some of these include:

- Providing ongoing cybersecurity training and consistent policies to all employees and students
- Integrating cybersecurity practices into classroom instruction
- Utilizing tools such as self-phishing campaigns to raise awareness and identify staff who need additional remedial training.
- Including cybersecurity and privacy responsibilities in position descriptions

Processes

Processes are the repeatable steps necessary to accomplish a district's educational and operational objectives. The development, documentation, training, and implementation of effective processes are a key step in managing an effective cybersecurity program. Examples of processes include:

- Conducting regular risk assessments to identify and prioritize risk.
- Developing, implementing, and auditing cybersecurity policies to set and enforce standards.
- Conducting cybersecurity audits, both internal and external.

- Build cybersecurity into the organization's decision-making processes, e.g., purchases, including cybersecurity messaging and information in newsletters, social media posts, etc.

Technology

Technology is the third element of a solid cybersecurity program. The technology element focuses on technologies that support the protection of the confidentiality, integrity, and availability of the data and systems the district is responsible for securing. Representative examples of initiatives in this area include:

- Automating employee onboarding and offboarding, including the assignment of rights and access
- Maintaining and managing internet filtering and monitoring systems
- Backing up systems for potential disaster recovery or business continuity scenarios

How do I start building my cybersecurity program?

Cybersecurity programs take time to nurture and grow. It is not possible to launch a fully built cybersecurity program overnight and, often, people struggle because they start too big instead of taking one intentional step at a time. Start with these three foundational steps for launching your cybersecurity program. These steps are not in a specific order, you may need to adjust the order to meet the specific needs of your district.

1. Obtain executive leadership support and sponsorship. Having a superintendent or deputy superintendent who is willing to be an active champion for cybersecurity will help elevate the program out of the technology department and make it a district initiative.
2. Conduct a third-party risk assessment or audit. Completing a third-party risk assessment or audit is not about blame or criticism, it is about establishing the district's current baseline and having a neutral third party provide a realistic assessment of the district's cybersecurity risks.
3. Establish a governance structure. When you start, your governance process may consist of a monthly meeting with 3-4 key district leaders. Engaging leaders from the district in governance will help to provide perspective on organizational risk tolerance, prioritization of work, and assistance with access to resources.

Setting Cybersecurity Program Goals

An essential element of successfully beginning a cybersecurity program is to outline key goals for the program. When establishing program goals, it is important to make sure that you start with a set of goals that are agreed upon, achievable, and can be accomplished within a designated time period.

The most effective way to set goals that align with your organizational objectives is to work with your governance team to identify and agree upon the goals. Taking this approach will also build support for your cybersecurity program and the specific goals and related tasks. One example goal might be to provide at least 30 minutes of training for all district personnel followed by a cybersecurity tips email message every term. Another more technical example goal might be to implement multi-factor authentication for technical and finance/HR staff.

Avoid setting too many goals. Intentionally limiting your program to two or three specific goals can set a foundation for success and improve the likelihood those goals are met. Remember any progress is an improvement, so set two to three goals that have meaning and move your program forward.

Make sure the program goals can be measured and report back to your governance team on progress toward achieving the goals. Communicating progress engages the governance team in the process and ensures an opportunity to share challenges, barriers, and opportunities with which you may need additional support or assistance.

Launching the program

Following these recommendations for designing and building a cybersecurity program will prepare you for launching your school district cybersecurity program. Strategize with the governance team to determine the best approach for communicating the launch of the cybersecurity program and the support of district leadership for this effort. Clearly communicating what the program includes and why the district is pursuing cybersecurity will support a successful launch.

Remember, as you launch your program that you're launching a continuous process improvement initiative and while specific goals and objectives will have deadlines and timelines, the program should adapt and adjust to align with your district's three-to-five-year plan and contain targeted goals for different audiences.