CoSN
LEADING EDUCATION INNOVATION

Strategies for Building Information Security Governance

Given the pervasive nature of cybersecurity security threats and attacks against school systems, it is not viable for IT Directors or Chief Technology Officers to be solely responsible for protecting schools and districts from cyber adversaries. Cybersecurity and cyber safety are not technical issues but organizational challenges that affect all members of the education community.

How do you transition from relying only on IT for cybersecurity and cyber safety? By introducing a cybersecurity governance practice into your organization, Governance is the means by which the organization determines and coordinates an approach to risk management and makes decisions.

Put more simply; Governance is making sure the organization is doing the right things. Governance provides oversight for IT, facilities, instructional design and curriculum, and more to ensure that cybersecurity risks are adequately mitigated, give clear direction on cybersecurity activities, and accept risk on behalf of the organization.

How do you build a governance structure?

Plenty of books will provide directions for building robust (and often overwhelming) governance structures. However, the key to successful governance implementation is to keep it simple at the start. Start small, and build the governance structure. It is possible that, based on the size and complexity of the school system, the governance structure will never need to be large.

1. Pick 3-4 key high-level leaders who are responsible for cybersecurity and cyber safety for the school system. This team of leaders could include any of the following: a School Board member, Superintendent

(or Designee), Assistant Superintendent(s), Finance Director, Communications Director, General Counsel, Curriculum Director, Risk Management, etc., and the CIO/CISO/CTO/Technology Director. Representation should include at least one member responsible for student learning outcomes and willing to assist in aligning cybersecurity with the curriculum.

2. Establish and agree to a regularly scheduled time to meet. Given busy schedules and scheduling challenges, a goal of one hour a month may be a realistic starting point.

3. Define clear roles and responsibilities. These may be quite simple such as:
    a. Chief Information Officer (CIO)/ Chief Information Security Officer (CISO(/ Chief Technology Officer (CTO)/Technology Director, Facilities Director, and others brief the governance team on the current state of cybersecurity in the school system, current cybersecurity initiatives, budget issues, options for mitigating or accepting specific risks, and provide decision points.
    b. Governance team makes decisions about risks to accept and projects/efforts to support to mitigate risks. This includes making budget decisions, determining who is responsible for implementation, and providing guidance on timing and communications.

4. Set agendas and provide supporting documentation in advance of each meeting.

The first governance meeting

The goal of the first meeting of the governance group should be to orient the members to cybersecurity in the school system. Prepare to discuss the following topics with the governance committee:

- Introduce the concepts of Governance and the role of the group in guiding the school system’s cybersecurity program
- Discuss the purpose and function of the governance group

    - Accountability vs. Responsibility - what is the difference and the role of the governance team?
    - Metrics - how will the group define and measure success?
    - Funding and budget – what is the responsibility of this group in identifying or providing funding for cybersecurity initiatives?
    - Decision-making process – how will the group make, document, and communicate decisions?
- Define risk and begin the discussion of risk tolerance
- Summarize the current state of cybersecurity and cyber safety in the school system in terms of risk. Do not go overboard on the technology.
- Have the governance committee identify their goals for cybersecurity and cyber safety in the school system.

Follow up governance meetings

Follow up meetings should be scheduled on a regular and realistic cadence. Recommendation would be once every month or once every two months. Subsequent meetings should focus on key items including, but not limited to:

- Approving a school system cybersecurity plan aligned with the goals identified by the governance group
- Reviewing and approving cybersecurity budgets, budget line items, and projects
- Identifying and recommending awareness and training strategies
- Educating the governance team about new and emerging cybersecurity threats
- Reviewing audits, cybersecurity initiative plans and completion status, and maintaining accountability for action on cybersecurity efforts
- Set a schedule to review and modify the cybersecurity program, policies and procedures on a regular (annual, quarterly, etc.) basis.
- Agree upon and set a regular cadence for reporting on the work the governance group is doing either to district leadership or to the school board.

Each follow up meeting should generate action items and next steps. The governance group should guide the development and evolution of the school system's cybersecurity posture and culture and help school system leaders understand their roles and responsibilities in building a strong cybersecurity and cyber safety foundation.

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