Empowering School IT Teams Through Cybersecurity Professional Development

CoSN Cybersecurity Committee

Introduction

In today's digital-first, AI-enabled educational landscape, cybersecurity is no longer optional; it is essential. For IT Directors in school districts, growing the cybersecurity capabilities of their IT teams isn't just a technical upgrade; it's a strategic investment in the safety, resilience, and future-readiness of the entire learning community. Cyber threats targeting schools are rising, from phishing scams and ransomware attacks to data breaches and evolving social engineering tactics. These incidents can disrupt learning, compromise sensitive data, and drain district resources.

Hiring cybersecurity professionals is difficult in a competitive marketplace, and training them internally offers financial challenges, as many cybersecurity training courses are expensive and time-consuming. However, by investing 1–2 hours per week in staff cybersecurity development, using existing free and low-cost training, IT Directors can build a proactive defense culture that benefits both the district and individual employees.

Building a district's cybersecurity capabilities through consistent staff training provides meaningful advantages:

- Reduced risk of breaches: Trained staff are better equipped to recognize and respond to threats.

- Faster remediation: When incidents do occur, knowledgeable staff can quickly identify issues and take prompt action to minimize their impact.
- Improved compliance: Many cybersecurity frameworks require ongoing training.
- Enhanced reputation: A district recognized for its strong digital security earns trust from parents, students, and the broader community.
- Operational continuity: Fewer incidents mean less downtime and disruption.

For staff:

- Increased staff morale: Investing in professional growth demonstrates to employees that they're valued, thereby boosting engagement and retention.
- Increased confidence: Staff feel empowered to manage digital tools securely.
- Professional recognition: Certifications and training can lead to promotions or new roles.
- Personal protection**:** Skills learned at work often translate to safer personal digital habits.

Making Time for Growth

Finding 1–2 hours a week for training may seem challenging, but it's achievable with intentional planning:

- **Schedule "Cyber Hours"**: Block out weekly time slots for staff to engage in learning.
- **Create learning cohorts**: Encourage peer support and accountability.
- **Incorporate into PD days**: Dedicate part of professional development sessions to cybersecurity.
- **Celebrate milestones**: Recognize staff who complete certifications or courses.

Cybersecurity Training Resources

Fortunately, high-quality cybersecurity training is available at no cost and low cost. The options below are ranked based on cost ($0 to $$) and complexity (★ - ★★★★). Here are some standout options:

Cybersecurity & Infrastructure Security Agency (CISA) Learning ($0, ★★)

Hosted by the Cybersecurity and Infrastructure Security Agency, CISA Learning offers free courses on cybersecurity best practices and critical infrastructure protection. It's ideal for school IT teams seeking to understand federal standards and enhance resilience across their systems.
https://niccs.cisa.gov/training/cisa-learning

COSN Cybersecurity & Privacy Workshops & Classes ($, ★★)

COSN offers a range of low-cost, online workshops and courses in key cybersecurity and privacy topics, including security planning, incident response, business continuity planning, and more. These courses are specifically designed for the K12 environment.

https://www.cosn.org/year-round-catalog/

CoSN Cybersecurity Rubric ($0, ★★)

With cybersecurity threats to schools continuing to escalate—and existing standards often too complex or costly for K–12 environments—CoSN is stepping forward to lead the next phase of the Cybersecurity Rubric. Originally developed by ClassLink and a coalition of education organizations through the Cybersecurity Coalition for Education (CC4E), the Rubric provided a much-needed, practical framework tailored specifically to schools.

https://www.cosn.org/cybersecurity-rubric/

Certified Information System Security Professional (CISSP) Mentor Program ($0, ★★★)

Offered by FRSecure, this free annual program helps learners prepare for the CISSP exam—a gold standard in cybersecurity certification. The mentor-led format includes weekly sessions, study materials, and community support. It's best suited for staff with some experience who want to deepen their expertise. The Mentor Program does not include the CISSP exam.
https://frsecure.com/cissp-mentor-program/

FEMA Incident Command Training ($0, ★)

While not strictly cybersecurity, FEMA's free courses on incident command systems are invaluable for understanding emergency response protocols. These skills complement cybersecurity readiness, especially in managing breaches or system failures.
https://www.firstrespondertraining.gov/frts/npccatalog

ISC2 Certified in Cybersecurity ($0, ★)

ISC2's "One Million Certified in Cybersecurity" initiative provides free training and certification exams for entry-level professionals. No prior experience is required, making it perfect for staff new to cybersecurity. Upon passing, participants join ISC2, gaining access to a global network and ongoing resources.
https://www.isc2.org/certifications/cc

Infragard ($0, ★★)

InfraGard offers free training through various programs, including the National Infrastructure Security and Resilience University (NISRU), which provides webinars and workshops for its members. Members also gain access to other complimentary or discounted resources, including the Security Awareness Training self-paced cybersecurity course, online training from CISA (such as Industrial Control Systems training), and collaborations with organizations like the FBI, DHS, and private sector partners.

Infragard membership is free. https://www.infragardnational.org/

SANS Cybersecurity Training ($0-$$$$, ★★★)

SANS offers a range of free training in addition to paid training and certification opportunities. SANS paid training and certifications represent a significant financial investment and are for more advanced cybersecurity professionals.

https://www.sans.org/mlp/cybersecurity-training-community
SANS also offers a range of advanced cybersecurity trainings that are not free. There are discounts for Education Organizations, but require to buy minimum of 3 courses at a reduced price: https://www.sans.org/partnerships/education

Webinars from CoSN, BrightTalk, and Others ($0, ★★)

Webinars offer bite-sized learning on current threats, tools, and strategies. Organizations like CoSN (Consortium for School Networking) and BrightTalk host frequent sessions tailored to education technology leaders. These are great for staying updated and sparking team discussions.

CoSN Webinars: https://www.cosn.org/education-events/event-calendar/ filter on webinars
CoSN Webinar Recordings @CoSNweb
CoSN Podcast Series
BrightTalk webinars

Professional Development Can Be Fun

Beyond formal training, there are a range of activities that can be used to build employee's knowledge and experience. Here are some examples of tools and methods:

- Incorporate hands-on tools such as board games and card games, for example, Backdoors & Breaches (https://play.backdoorsandbreaches.com/), and play a game once a month.
    - Have a Free Friday afternoon or a lunch event for your staff where they play a game
    - Use the CoSN cybersecurity game online
- Host Password Check Day - All staff go to Password Checker and enter something similar to their current personal passwords/work password and see how long it would take hackers to hack. Declare a winner based on whose password will take the longest to brute force. Use this as an icebreaker to start a conversation about safety.
- Host a tabletop exercise

Model the Professional Development You Want to See

Professional development isn't just about individual growth; it's about creating a culture. CIOs, CTOs, and IT Directors can lead by example by:

- Sharing personal learning goals.
- Advocating for cybersecurity engagement with the district leadership and board of education.
- Encouraging cross-departmental participation.
- Integrating cybersecurity into everyday conversations.
- Attending local and national conferences

Cybersecurity is a shared responsibility, and IT leaders are uniquely positioned to champion it. By carving out small, consistent learning opportunities and using free or low-cost resources, school IT leaders can build resilient teams and safer digital environments. Even starting with one training activity or one weekly can lay the foundation for a culture of awareness, curiosity, and continuous improvement.

CoSN is vendor neutral and does not endorse products or services. Any mention of a specific solution is for contextual purposes.