How to Hire Cybersecurity Staff in K12

from the CoSN Cybersecurity Committee

K12 schools and districts have traditionally focused on providing connectivity and access to online resources. However, the shift towards securing these connections and protecting data has created a need for specialized cybersecurity roles. Schools must recognize that cybersecurity is not just a technical issue but a comprehensive challenge that involves people, processes, and technology.

Hiring cybersecurity staff in K12 education is a critical task that requires a strategic approach to ensure the safety and security of student data and school systems. The following recommendations will help you recruit cybersecurity professionals in K12 settings. Not sure how to get started determining the cybersecurity staffing needs for your district? Work with your Education Service Agency to partner on a position to support multiple small districts, hire a vCISO (virtual Chief Information Security Officer), take advantage of the no-cost CIS Cybersecurity Advisory Services Program, or outside consultant to design position descriptions and/or evaluate applicants.

1. Develop Clearly Scoped and Dedicated Cybersecurity Positions

Creating dedicated cybersecurity positions offers several advantages, including specialized training and experience in managing and responding to cyber threats. Schools should assess their specific needs and design focused position descriptions that align with their requirements. Avoid creating a position description that contains every component of cybersecurity, and make sure the position description is focused on a specific area.

Key areas of focus include leadership and management, network and systems defense, security operations, and incident response. It is important to note that one position cannot cover all areas of cybersecurity, and while this position is a specialist, cybersecurity is the responsibility of all district employees. Schools will need to have other staff members who can learn and take on some of the cybersecurity responsibilities, designate responsibilities of existing positions, or consider additional positions.

2. Avoid Overloading Applicant Requirements

It's important not to bloat the requirements for your cybersecurity positions. For example, when hiring entry level positions or positions in areas with limited populations, schools and districts can't afford to look for a unicorn with 5-10 years of experience and a degree in the field for an entry-level salary.

Instead, make reasonable entry-level requirements that will net you someone with training and education but maybe not as much experience. Value their lived experience including previous work history, military service, and/or formal education (certifications or degrees) and

focus on their people skills, learning capability, and potential to grow within the role.

Example entry-level requirements include:

- Minimum 2 years of experience in working in information technology, or associate degree or bachelor's degree in technology, or industry certifications listed below, or combination of relevant education and experience.
- Certification (for example, Security+, ISC2 CC, etc.) within X months of hire. The district commits resources to the certification process.
- Knowledge of cybersecurity principles and frameworks (e.g., NIST, CIS Controls) and ability to apply them to real world.
- Technology experience in any of the following areas: cybersecurity tools and techniques, networking, enterprise systems administration, server administration, or cloud computing operations.
- Strong problem-solving, communication, customer service, and project management skills.
- Ability to work independently, handle confidential matters, and meet deadlines.
- Ability to learn new technologies and successfully complete vendor specific training.
- Commitment to cultural competence and equity.

Invite applicants by casting a wide net and encouraging people to apply. Many talented and capable potential applicants won't apply for a

position unless they think they meet all the qualifications. Include a statement in your postings that acknowledges this and encourages people to apply. Here is an example:

We recognize that many individuals, including women and minorities, may hesitate to apply for a position unless they meet every requirement. If you meet most of the qualifications and are passionate about this role, we encourage you to apply.

3. Plan for Ongoing Professional Development

Cybersecurity is a rapidly evolving field, and continuous professional development is essential for maintaining up-to-date skills. Schools must budget for ongoing training and certifications for their cybersecurity staff to ensure they remain effective in their roles. Emphasize support and funding for ongoing professional development in your position posts.

4. Build Talent Pipelines Through Local Partnerships and Programs

Collaborate with local educational organizations, such as Cyber Clinics and similar programs, to connect with skilled individuals and recent graduates. By leveraging internships and apprenticeships, you can identify top talent and cultivate potential hires who align with your organization's needs.

Conclusion

Hiring cybersecurity staff in K12 education requires a multifaceted approach that includes developing dedicated positions, integrating

responsibilities into existing roles, leveraging external resources, and fostering a culture of cybersecurity through training and awareness.

Schools and districts need to be creative and adaptable in their hiring practices. Offering more than just a salary, they should emphasize the connection to the mission, provide opportunities for professional development, and create a great work environment. By following these guidelines and setting realistic expectations for applicants, schools can build a robust cybersecurity framework that protects their data and systems.

Additionally, hire for the capability to do the work, willingness to learn and grow into the work, problem solving skills, positive attitude and ability to work well with others. Technical skills can be trained, good people skills are much harder to train. Don't try to find someone who already knows all the technology.

Samples

https://docs.google.com/document/d/1AUtx-_jVa7BTXaYmj8Ih1DlYkEiC4U1x8vbJjGCA2Ac/edit

https://docs.google.com/document/d/1AygKvJKjI5KJD0PqoKUkhXGSOrpDaqJ2mptZK9zPyJk/edit

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

About The Consortium for School Networking

CoSN, the world-class professional association for K-12 EdTech leaders, stands at the forefront of education innovation. We are driven by a mission to equip current and aspiring K-12 education technology leaders, their teams, and school districts with the community, knowledge, and professional development they need to cultivate

engaging learning environments. Our vision is rooted in a future where every learner reaches their unique potential, guided by our community. CoSN represents over 2050 school districts reaching over 11 million students. Our state presence is expanding with 33 CoSN Chapters in 34 states who function at the grassroots level to further effect change and continues to grow as a powerful and influential voice in K-12 education.

CoSN also provides opportunities for companies that support the K-12 EdTech community to participate as corporate members.

Published Jan. 2025