command much higher salaries in industry than many schools and districts can afford. While outside consulting services can help bridge the gap, schools and districts should invest in technical staff to ensure their IT security skills are kept current. It is also important for schools and districts to educate faculty, staff, and students about best practices in cybersecurity and data protection. Training users to create complex passwords, identify phishing emails, and recognize suspicious websites can pay huge dividends in network security. Additional training about specific federal and state privacy legislation impacting education and basic data security best practices can help prevent the inadvertent release of confidential information. Most important is developing a culture that emphasizes the thoughtful implementation of security policies rather than mere compliance—a culture in which cyber- and data security are seen as a community responsibility. A well-trained and security-aware workforce is one of the best defenses organizations have against data breaches and malicious attacks. Similarly, it is critical to provide students with training.

MAKING EMPLOYEE CYBERSECURITY EDUCATION A PRIORITY

The Madeira School in McLean, VA decided to make employee cybersecurity education a priority after 40 percent of its employees "fell" for a simulated phishing attack sent by an outside security vendor contracted by the school. Further data analysis showed that 80 percent of new employees (hired within the past year) fell for the phishing simulation. Jeff Dayton, Director of Technology and Innovation, immediately began working with the human resources department to incorporate cybersecurity training into the new employee onboarding process and teacher professional development. He created a cybersecurity-focused intranet website for employees that houses the school's technology and data security policies and contains links to videos, news articles, and other cybersecurity education resources. Dayton also conducted an internal cybersecurity audit using an auditing checklist available online to identify security gaps with regard to policies and technology. He is using the audit results to systematically mitigate potential security risks.

Dayton began publishing a weekly email security newsletter for faculty and staff, drawing topics from the week's headlines and conversations with staff. For example, during March Madness, he wrote about basketball tournament-related cyber scams. By relating content to current events and their personal interests, Dayton finds that users are more likely to engage with the shared resources.

Policies: Clear and well-communicated policies around cybersecurity and data privacy are another important component of a well-implemented security program. These include policies addressing technical practices such as network security and access control, data backups and retention, password management, mobile device policies, and incident response as well as policies regarding such topics as confidential data access, data transfer, data sharing, and encryption. Schools and districts that accept credit cards may have to develop additional security policies and procedures, such as those for Payment Card Industry Data Security Standard (PCI-DSS) compliance.

Policies should be reviewed and updated on a regular basis and outlined in a school or district's cybersecurity plan or cybersecurity annex that is part of a larger Emergency Operations Plan. Inform employees and users about policy requirements. Be sensitive to the fact that policies that make sense on paper may present challenges in practice in an educational environment. Balancing these security considerations with educational needs and impact to students and