Cybersecurity guidance, questions and resources for school governance teams

Background

Cybercrime is on the rise across the country and, increasingly, public schools are the target of sophisticated attacks that capture sensitive data, violate privacy, dismantle operations and extort funds from school districts and county offices of education.

Ransomware attacks have grown in recent years and schools have increasingly been identified as soft targets lacking the capacity to ward off hackers. In addition, greater reliance on technology to deliver instruction and services since the COVID-19 pandemic has left schools increasingly vulnerable to cyberattacks.

In 2022, cyberattacks grew by 150 percent, with the average attack lasting 66 hours. Cyberattacks against the education sector increased by 36 percent. For local educational agencies, it is not a matter of if — but when — your school information systems will be subject to a cyberattack, which can render the entire school district or county office of education unable to conduct the day-to-day business of educating students.

While local educational agencies are doing their best to combat these threats, most education IT departments are understaffed and have limited resources, which is why CSBA is sponsoring Assembly Bill 1023 (Papan, D-San Mateo) to provide LEAs with resources to defend against cyberattacks and protect sensitive data for students, staff and families.

Gov. Gavin Newsom has proposed funding in this year's budget to enhance the California Cybersecurity Integration Center (Cal-CSIC), but this support is not specific to TK-12 and the statutory language could be used to exclude schools from cybersecurity funding. CSBA-sponsored AB 1023 would ensure that state agencies are required to provide direct cybersecurity assistance to TK-12 schools, allowing them to prepare for and respond to cyberattacks more effectively.

Yet, in addition to accessing support from the state, there is much boards of education can do at the local level to help guard against and mitigate the severity of cyberattacks. This list of tips and resources is intended to guide you in the right direction.

Questions for board members to consider:

- Where do we stand in terms of preparedness for a cybersecurity attack?
- What does the board need to know about disaster recovery?
- How long will it take the LEA to recover from an attack?
- Do we have adequate cybersecurity insurance?
- How long do we have to retain data? How often do we purge sensitive files?

Questions for IT staff:

- What do you need to secure the LEA?
- Have you reviewed the Instant Response Plan with the board?
- Does our plan align with our insurance carrier requirements?
- Who can the LEA turn to for an IT security audit?

Guidance: Key steps to protect your data

Preparing for cyberattacks

- Develop a comprehensive cybersecurity policy and procedures manual
- Conduct regular cybersecurity risk assessments to identify vulnerabilities
- Implement strong password policies and enforce regular password changes
- Provide ongoing cybersecurity training for staff, students and parents
- Establish a system for monitoring and logging network activity
- Regularly update and patch software systems and applications
- Backup critical data and ensure it is stored securely

Defending against cyberattacks

- Install and maintain updated antivirus and antimalware software
- Utilize firewalls and secure network configurations
- Implement multi-factor authentication for all user accounts
- Restrict administrative access and privileges
- Enable automatic software updates and security patches
- Regularly scan and monitor the network for anomalies and intrusions
- Establish incident response protocols and communication channels

Mitigating cyberattacks

- Develop and practice an incident response plan for cyberattacks
- Establish a dedicated incident response team with assigned roles
- Isolate compromised systems to prevent the spread of attacks
- Engage with law enforcement and cybersecurity experts when necessary
- Communicate promptly and transparently with stakeholders about the incident
- Analyze the attack, learn from it, and update security measures accordingly
- Conduct regular post-incident reviews and debriefing

Resources

National Institute of Standards and Technology (NIST) Cybersecurity Framework: www.nist.gov/cyberframework

U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) K-12 Cybersecurity Resource Center: www.cisa.gov/k-12-cybersecurity

Federal Bureau of Investigation (FBI) Cyber Crime Unit: www.fbi.gov/investigate/cyber

California Cybersecurity Integration Center: www.caloes.ca.gov/office-of-the-director/operations/homeland-security/california-cybersecurity-integration-center/

National Cybersecurity Alliance (NCSA): www.staysafeonline.org

Information Sharing and Analysis Centers (ISACs) for Education: www.isao.org/isao/isao-education

Cybersecurity & Infrastructure Security Agency (CISA): www.cisa.gov/

Center for Internet Security (CIS): www.cisecurity.org/about-us

Corporation for Education Network Initiatives In California (CENIC): https://cenic.org/

Carahsoft: www.carahsoft.com/solve/cybersecurity