On The Alert!

Date: January 13, 2023
Attention: ASCIP Members
Affected Department(s): Risk Management, Admin, Teachers, & Staff
Applicability: K-12 School Districts & Charter Schools

CALIFORNIA SCHOOL CYBERSECURITY ACT AND DISTRICT RISK

Effective January 1, 2023, Assembly Bill 2355 (AB 2355), also known as the California School Cybersecurity Act, requires school districts and charter schools to report cyberattacks impacting more than 500 pupils or personnel to the California Cybersecurity Integration Center (Cal-CSIC) at (833) REPORT-1 or calcsic@caloes.ca.gov. The purpose of this law is to help ensure that K-12 schools in California are better equipped to protect student data and prevent future cyberattacks.

AB 2355 does not specifically favor any technological solutions for improving cybersecurity in K-12 schools in California and allows each district to determine the most appropriate technological solutions for improving cybersecurity and protecting student data. As a general principle, it is important for schools to implement a variety of measures to improve cybersecurity and protect against cyberattacks. At minimum, ASCIP recommends that districts implement the following security measures:

- NETWORK BACKUP: Conduct regular network server backups and store them off-site (preferably via a cloud service) and the backups are accessible only via unique credentials
- MULTI-FACTOR AUTHENTICATION (MFA) FOR REMOTE NETWORK ACCESS: Use an approved multi-factor authentication application for users to access the network remotely.
- END-POINT DETECTION & RESPONSE: Implement a suite of security protections including anti-virus, firewall, malware, device management, etc. (typically via a third-party service).

School districts and charter schools can subscribe to the California Department of Education’s (CDEs) it-security-tips mailing list by sending a blank email to join-it-security-tips@mlist.cde.ca.gov to receive additional cybersecurity information.

ASCIP Cybersecurity Protections: ASCIP offers a suite of cybersecurity protections1 to its members including:

- **Cyber Education & Awareness:** The Cyber Education and Awareness series includes training on:
  - general user cybersecurity awareness,
  - phishing campaigns and education (NEW!), and
  - disaster recovery
- **Cybersecurity Incident Response Planning:** Members using this service can take advantage of a structured approach to creating an Incident Response Plan. Also offered are tabletop exercises designed to train and assist members in working through a possible incident scenario.
- **Cyber Risk & Vulnerability Assessment:** The Cybersecurity Risk Assessment process is the initial step in helping districts understand threats to and vulnerabilities of their information systems. This service begins with a risk assessment survey and provides a prioritized list of risks.
- **IT Policy Templates:** Districts can download templates from ASCIP’s Cybersecurity Member Portal.

---

1 See https://www.ascip.org/risk-resources/cyber-security/

*Please contact your ASCIP risk services consultant at (562) 404-8029 to discuss further.*