ALLIANCE OF SCHOOLS FOR COOPERATIVE INSURANCE PROGRAMS

ASCIP

On the Alert!

Date: September 1, 2022

Attention: ASCIP Members

Affected: Risk Management, Information Technology, Administration

Applicability: Community College Districts, K-12 Districts & Charter Schools

CYBER ATTACKS AND IMMINENT DISTRICT RISK

In the past six months, two ASCIP Community College members have been victims of cyber-attacks. Through phishing emails to employees, they plant malware, allowing them to access the district's system then locate and copy high value files across the network (i.e. SSNs, medical information, and classified student data). After copying files, they encrypt data on the district's server and delete backups, rendering systems inaccessible and severely disrupting operations. Then the criminals demand a ransom payment and threaten to publish the data if the ransom is not paid. These hackers have been observant of the district's reactions to their attacks and have quickly incorporated new tools in response.

Districts must implement cyber security protections to defend against such attacks. At a minimum:

Network Backup: Conduct regular network server backups and store them offsite (preferably via a cloud service). The backups should only be accessible via unique credentials.

Remote Network Access: Utilize an approved multi-factor authentication application for users to access the network remotely.

End-point Protection & Response: Implement a suite of security protections, including anti-virus, firewall, malware, device management, etc., via a third-party service.

ASCIP Cyber Security Resources

To help members meet the evolving nature of cyber threats, ASCIP significantly expanded its cyber security resources this past year. These resources include:

- Cyber Risk & Vulnerability Assessments
- Cybersecurity Incident Response Planning
- Virtual Chief Information Security Officer (vCISO) Services
- Cyber Education and Awareness
- IT Policy Templates, including Incident Response Plans
- Breach Table-Top Drills

Additionally, the Cybersecurity and Infrastructure Security Agency (CISA), in collaboration with the Federal Bureau of Investigation (FBI), has developed the following fact sheet for cyber threats to school districts for remote learning education: Cyber Threats to K-12 Remote Learning Education.[1]

ASCIP Assistance When Breaches Occur

ASCIP offers forensic analysis to uncover how breaches occurred, legal advice on what to do next (notifications, credit monitoring, and more), public relations guidance, insurance support for financial losses, and expert advice on prevention.

Please contact your ASCIP Risk Services Consultant or our Risk Services team at RM_Info@ascip.org for questions or to discuss further.

[1] See https://www.cisa.gov/stopransomware/cyber-threats-k-12-remote-learning-education