ALLIANCE OF SCHOOLS FOR COOPERATIVE INSURANCE PROGRAMS

ASCIP

On The Alert!

Date: October 15, 2021
Attention: ASCIP Members
Affected Department(s): Risk Management, Tech. Services, Admin, & Staff
Applicability: K-12 Districts & Charter Schools

K-12 CYBERSECURITY ACT OF 2021 & DISTRICT RISK

On Friday, October 8, 2021, President Biden signed into law S. 1917, the "**K-12 Cybersecurity Act of 2021**," which requires the Cybersecurity and Infrastructure Security Agency (CISA) to study the cybersecurity risks facing elementary and secondary schools and develop recommendations that include voluntary guidelines designed to assist schools in facing those risks.[1]

Malicious cyber actors have increasingly targeted school computer systems by many techniques including:

- slowing access,
- rendering systems inaccessible to basic functions, including remote learning,
- stealing or threatening to steal or leak confidential student data unless a ransom is paid (**ransomware**),
- disrupting live-conferenced classroom settings by verbally harassing students,
- displaying pornography and violent images, or
- publicly revealing previously private personal information about an individual or organization (**doxing**).

Reducing the Threat of Ransomware

Among the most potentially harmful acts is ransomware. Ransomware is a type of malicious computer software that threatens to publish the victim's personal data or perpetually block access to it unless a ransom is paid. More advanced ransonware uses a technique called cryptoviral extortion that encrypts the victim's files, renders them inaccessible, and demands a ransom payment for decryption. In a cryptoviral extortion attack, recovery of the files without the decryption key is an intractable problem, and difficult to trace digital currencies that are used for paying ransoms make tracing and prosecuting the perpetrators difficult.

Due to the rise in malicious activity with ransomware attacks against K-12 educational institutions since the onset of COVID-19 and the increase in remote learning, CISA, in collaboration with the FBI, has produced a fact sheet, **Cyber Threats to K-12 Remote Learning Education**.[2]

ASCIP Cybersecurity Protections

ASCIP offers a suite of cybersecurity protections[3] to its members including:

Tests for Vulnerabilities
ASCIP helps members by offering cybersecurity assessments to test members' systems for vulnerabilities and by providing recommendations for increasing security.

Resources for Cybersecurity
ASCIP offers training, best practices, and policy templates to increase cybersecurity.

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.

---

[1] See https://www.whitehouse.gov/briefing-room/statements-releases/2021/10/08/bills-signed-s-1828-and-s-1917/ .
[2] See https://www.cisa.gov/sites/default/files/publications/Cyber_Threats_to_K-12_Remote_Learning_Fact_Sheet_15_Dec_508.pdf .
[3] See https://ascip.org/risk-services/risk-management-prevention-services-revised/ .

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