ALLIANCE OF SCHOOLS FOR COOPERATIVE INSURANCE PROGRAMS

ASCIP

On The Alert!

Date: August 26, 2019
Attention: ASCIP Members
Affected Areas: Risk Management & Information Technology (IT)
Applicability: K-12 Districts & Charter Schools

STATE OF EMERGENCY – CYBERSECURITY INCIDENT

On July 24, 2019, Louisiana Governor John Bel Edwards issued a state-wide Emergency Declaration in response to a cybersecurity incident that affected several local government agencies, including several school districts. Cybersecurity incidents seem to be a common occurrence. According to the State of K-12 Cybersecurity, a U.S. school district becomes the victim of a cyber-attack almost as often as every three days. They include data breaches, phishing scams, and ransomware attacks. According to Doug Levin, author of "The State of K-12 Cybersecurity: 2018 Year in Review", this figure represents only the tip of the iceberg. Therefore, school districts need to bolster their efforts towards preventing these types of incidents.

RECOMMENDED ACTIONS

Districts and charter schools should implement a data breach response plan and a cybersecurity risk management program. These programs should take into account processes that protect data systems by engaging in a continuous cycle of assessing for risk vulnerabilities, detecting potential threats, providing education, and training and timely responding to attacks and recovery efforts. Other actions to consider include:

- Conduct security audits to identify weaknesses and update/patch vulnerable systems
  - Security audits such as vulnerability scans should be conducted on an annual basis & proceed as a continuous security improvement
  - Test patches & upgrades before implanting into production
- Create and routinely review audit logs for suspicious activity, and retain as needed
- Train staff and students on data security best practices and how to recognize social engineering tactics by scammers
  - Raise awareness by conducting random phishing tests & provide online training to identify fraudulent or malicious emails and phone calls
- Limit access to sensitive data
  - Provide access on an as needed basis
  - Encrypt sensitive information when data at rest or in motion

RESOURCES

- https://k12cybersecure.com/resources/
- U.S. Department of Education. "Security Best Practices." Privacy Technical Assistance Center (PTAC) and the Family Policy Compliance Office (FPCO).
- Consortium for School Networking (CoSN). "Cybersecurity for the Digital District, a CoSN Leadership Initiative" *(Note: some resources require log-in/membership to access)*
- https://studentprivacy.ed.gov/

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