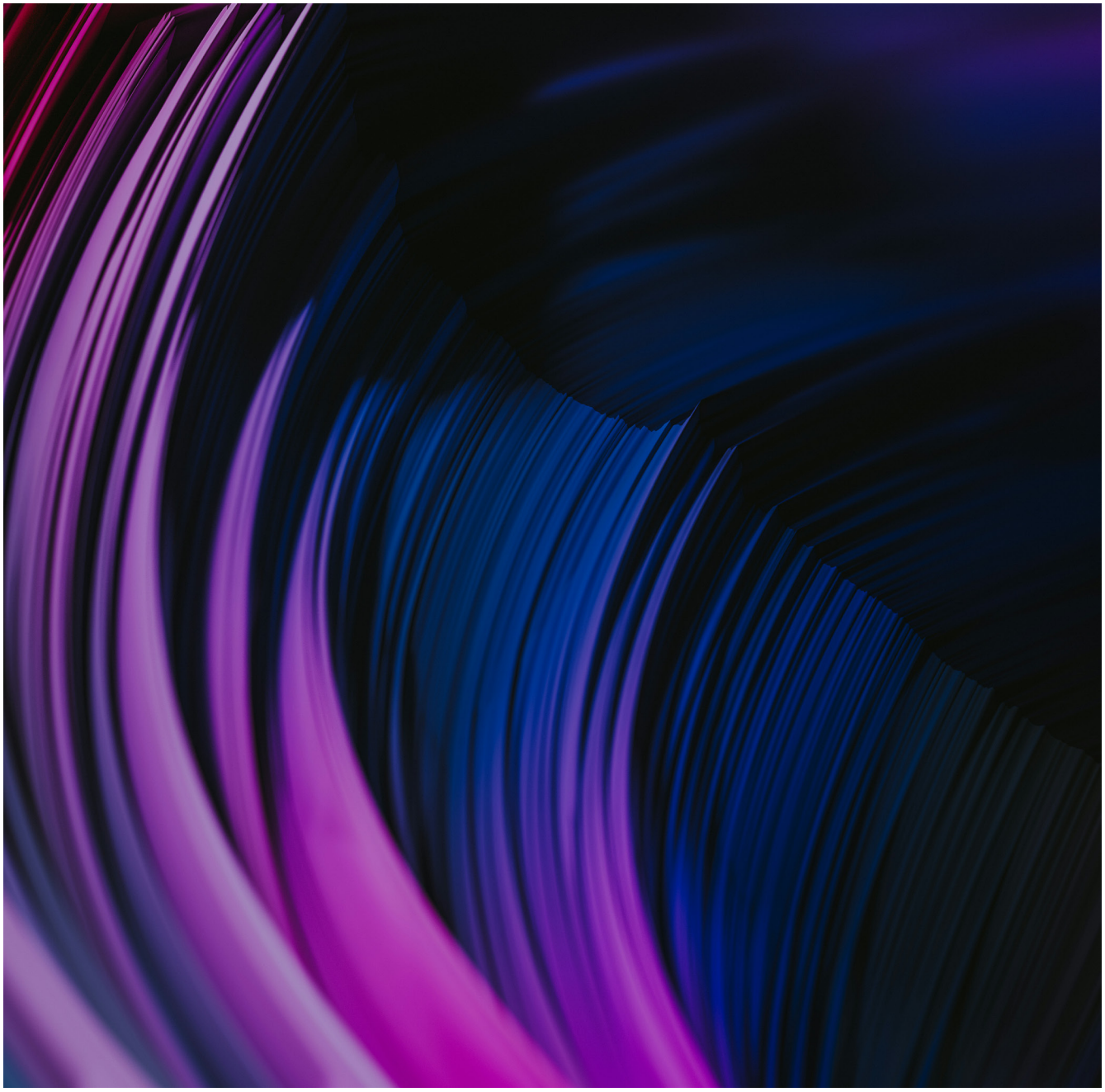

Cybersecurity:
Top Considerations For Cybersecurity Insurance

Cybersecurity

CITE™
CALIFORNIA IT IN EDUCATION

May 2025

www.cite.org

CITE™
CALIFORNIA IT IN EDUCATION

Cybersecurity:
Top Considerations For Cybersecurity Insurance

Multi-Factor Authorization (MFA)
Insurers heavily emphasize MFA implementation across all user accounts, especially those with administrative privileges. This is a primary defense against unauthorized access.

Cybersecurity Training
Regular employee & student training on cybersecurity best practices, phishing awareness, & safe online behavior is crucial for preventing human error, a significant cause of breaches.

Intrusion Prevention Systems (IPS)
Systems like next-generation firewalls are crucial for actively blocking malicious network activity and potential cyberattacks before they infiltrate school systems.

Network Access Control (NAC) & Segmentation
Implement network design & security policies that limit access to authorized users/devices and will minimize the spread of malware across sensitive data or systems.

Managed Detection & Response (MDR)
Managed Detection & Response (MDR) provides 24/7 monitoring and expert-driven threat analysis, detection, and response, significantly improving your security posture.

Patch Management & Vulnerability Scanning
Consistent system updating & vulnerability scanning are essential practices that proactively identify and remediate software flaws, preventing exploitation by attackers.

Backup Data & Recovery
Regular, secure, & immutable data backups are crucial in safeguarding sensitive information. Proactive testing ensures swift system recovery from data loss events.

Cyber Incident Response Planning (CIRP)
Having a well-defined Cyber Incident Response Plan enables you to react quickly while minimizing the damage and disruption from a cyberattack.

Related CITE Cybersecurity Resources
www.cite.org/cite-cybersecurity