CoSN
LEADING EDUCATION INNOVATION
cosn.org

THE IMPORTANCE OF CYBERSECURITY

With the increasing concerns about security among families, districts, and legislators, and with increased teacher and student reliance on internet accessibility, school cybersecurity is subject to more scrutiny than ever. Alarmingly, many districts are not being sufficiently aggressive in getting ahead of cybersecurity problems.

BELOW ARE THE TOP 5 REASONS WHY DISTRICT TECH LEADERS MUST MAKE CYBERSECURITY A PRIORITY.

1

LIABILITY

Districts and technology leaders may be held liable for network security incidents. The costs of these incidents can be extremely high and can include the cost of determining the cause, the cost of preventing future breaches, the cost of legal counsel, the cost of public relations to regain trust, and the cost of remediation. In the case of Ransomware, there may be the cost of ransom itself if the district chooses to pay, though that is often not recommended by law enforcement. Further, district tech leaders as individuals may be sued by families whose data was compromised by a security breach.

2

LEGAL REQUIREMENTS

Depending on the state, there may be legal requirements for how data is secured, generally requiring reasonable security measures. As concerns about data privacy continues to ratchet up, more state-level legislative action is being taken, which is creating a patchwork of privacy laws including suggestions for such restrictive laws as requiring districts to keep all data stored within the state. At the federal level, regulators require "reasonable security," leaving the data holder to determine what that requires, depending on security standards, best practices, and the sensitivity of the data.

3

PROFESSIONAL REPUTATION

The reputation of both the district and the technology leader are damaged when the network or district data are compromised. Network breaches often become the subject of media focus, creating a much bigger public relations disaster and leading to reputations being widely compromised.

4

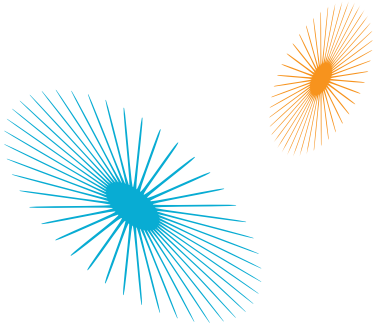
TEACHING AND LEARNING

When the network is unavailable, as with a Distributed Denial of Service (DDOS) attack, schools lose precious instructional hours. Teachers who are prepared to use technology in the classroom need to take the time to find and fall back on non-digital resources.

5

STUDENT DIGITAL RECORDS

Student records may be breached and maliciously modified. The risk is not only external hackers, but students themselves. Breached student records may negatively impact future college applications or employment. Student identities may be stolen with no one the wiser until the students apply for college financial aid.



CyberSecurity
for the digital district • a CoSN leadership initiative

THE EMPOWERED SUPERINTENDENT