The Importance of Cybersecurity

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

TOP 5 REASONS why school system tech leaders must make cybersecurity a priority

1 • Liability

School systems 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, preventing future breaches, legal counsel, public relations to regain trust, and remediation. In the case of ransomware, there may be the cost of ransom itself if the school system chooses to pay, though that is often not recommended by law enforcement. Further, school system 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 continue to multiply, more state-level legislative action is being taken, creating a patchwork of privacy and security laws nationwide. Some of these laws are more restrictive than others, with some requiring school systems 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 their systems security standards, best practices, and sensitivity of the data.

3 • Professional reputation

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

The Cybersecurity initiative is a CoSN focus area. For a comprehensive collection of downloadable resources, toolkits, and more, go to **https://www.cosn.org/edtech-topics/cybersecurity/**.