5 REASONS SCHOOLS MUST PRIORITIZE CYBER SECURITY

During the pandemic, schools have quickly become one of the favored targets of cyber criminals. This doesn't come as a surprise, as many districts are limited by budgets and have had to rush their adoption of new digital technologies, increasing the risk of a successful breach or cyber attack. In this new normal, school leaders must learn how to take appropriate actions against these threats to ensure the safety of students, staff, parents, and administrators.

We're going to look at the top five reasons why school districts must make cyber security their #1 priority.

> "The shift to remote learning opens the door for different points of attack that most school districts weren't prepared to support."

Liability

Districts and technology leaders may be held liable for network security incidents, and the costs of these incidents can be extremely high. District tech leaders as individuals may be sued by families whose data was compromised by a data breach. This is why it's recommended that school districts have cyber security insurance coverage.

However, the financial and legal issues that may result from a data breach aren't the only problems. When business operations come to a screeching halt, teachers can't hold their regular classroom sessions, and that is a significant liability on its own. Teachers' schedules are pushed back, and students lose out on valuable learning opportunities.

Legal Requirements

Here's a short list of several requirements that schools must abide by: FERPA, COPPA, CIPA, PPRA, and GDPR. When we look at these laws, it begins to look like alphabet soup. So how do you manage this all these complex regulations?

The key is to appoint someone to stay updated on all these changing requirements and guidance. For example, appoint a data protection officer, or have your CTO serve as the go-to person. Have that person keep you informed and educate the community on how you're remaining compliant.

You also want this appointed person to make sure any programs and applications that teachers install meet all the requirements. With so many districts engaged in distant learning, teachers may try to use any tool they can find to assist them with their online teaching, which expands the attack surface.

Reputation

> "It takes 20 years to build a reputation and five minutes to ruin it. If you think about that, you'll do things differently." – Warren Buffet

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 major public relations disaster which leads to reputations being widely compromised. All it takes is one incident to gain traction in the media for people to begin questioning your credibility in the education space.

Right now, people expect superintendents and school districts to be absolutely stellar in their approach to cyber security, with little room for error. This is why maintaining a pristine reputation is paramount.

Teaching and Learning

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

The reality is that when networks are down, or even when particular services or apps are down, then it really pushes teachers over the edge. In the traditional classroom setting, if the lesson wasn't working as intended, you just pulled students together and did a read aloud or performed collaborative group work. Now, if the network goes down, you really can't continue teaching, and many valuable teaching hours are lost.

Student Digital Records

> "Protecting data is much less costly than dealing with a security breach in which records are exposed and potentially misused."

Breached student records may be maliciously modified, negatively impacting students' future college applications or employment. When student identities are stolen during elementary or secondary school years, no one may be the wiser until the students apply for college financial aid.

Schools also need to protect students' locations and addresses. You don't want that information out in the wrong hands where it could be a safety concern, especially if you have students who come from abusive households, domestic violence situations, or are in witness protection programs.

Not only do you have to be secure in handling digital records, you must also ensure that the vendors who handle student records are following proper security protocols.

For additional information on the importance of cyber security in today's learning environments, visit edWeb.