PowerSchool

DIGITAL CHECKLIST:

Is Your District Ready for Cybersecurity Threats this Back to School?

ASSESS YOUR CURRENT CYBERSECURITY READINESS FOR REMOTE AND IN-SCHOOL OPERATIONS BY ASKING THESE QUESTIONS

With the shift to online teaching, learning, and operations, **cybersecurity threats have increased in K-12 schools and districts**. More users are working outside of the physical school, where there's far less control over security, which exposes districts to numerous new points of attack that they weren't previously set up to support.

Plus, many districts don't have full-time employees dedicated to cybersecurity, highlighting the need to effectively inform and train all users, including students, teachers, administrators, and even parents. By doing so, you're helping **build a culture of data protection for a secure future**.

Take this quick cybersecurity assessment to see if your school or district is ready to operate securely in a blended learning environment.

Learning at Home

Students and parents need secure access and clear instructions on how to operate safely in a remote environment.

OUR SCHOOL OR DISTRICT:

- ☐ Device usage and content filtering options to protect devices being used remotely
- ☐ An Inventory checklist for devices you distribute, including administrative rights
- ☐ Rules and guidelines for secure video sharing that accounts for encryption, storage, and privacy concerns
- ☐ Clear guidelines communicated about which software and tools are okay to use and which ones aren't, ensuring you're partnering with legitimate, trusted edtech vendors
- ☐ Tested firewalls, and antivirus and anti-malware software installed on each device to protect data, privacy, and equipment
- ☐ A system in place for how to handle password resets for users at home, including whether or not self-service options should be available

0 /6 Number of Boxes Checked

LEARN MORE: Get 5 Cybersecurity Tips for COVID-19 and Beyond >

Student & Staff Security Training

Ensure that staff, students, and parents are aware of the wide array of cybersecurity threats. Communicate regularly either from the IT department, each school's principal, or the superintendent.

OUR SCHOOL OR DISTRICT:

- ☐ Provides cybersecurity training for staff, students, and parents
- ☐ Distributes documented guidelines and policies for responsible use of software, devices, and platforms to help promote good digital citizenship
- ☐ Makes information and resources on data safety easily accessible
- ☐ Has a transparent response process to attacks involving students—what are your immediate and long-term steps if (and when) you are attacked to minimize risk to students?
- ☐ Communicates rules for accessing confidential work on unsecured networks (with public WiFi access)

0 /5 Number of Boxes Checked

LEARN MORE: Top 4 K-12 Cybersecurity Threats to Watch >

Safe Student & Staff Data Practices

Keeping the sensitive data of students and staff secure should be a top priority at all times. When data is hacked, it can cause both financial and emotional damage.

OUR SCHOOL OR DISTRICT:

- ☐ Follows an established schedule for updates, backups, and patches
- ☐ Has key software systems hosted through the vendor to reduce risk and foster an efficient, reliable, secure, and responsive environment
- ☐ Ensure vendors practice safe data practices. **Check to make sure they:**
- ☐ - Feature a credentialed chief information security officer (CISO)
- ☐ - Comply with regulations including FERPA, HIPPA, the Children's Online Privacy Protection Act, Breach Laws, Data Residency Laws, the Digital Millennium Copyright Law, the Sarbanes-Oxley Act
- ☐ - Signed the national Student Privacy Pledge
- ☐ - Achieved ISO/IEC 27001:2013 certification, renewed each year
- ☐ - Comply with the SOC 2® (Security Operations Center) examination

0 /8 Number of Boxes Checked

LEARN MORE: K-12 Data Security Tips from a CISO >

Planning for a Cybersecurity Attack

Preparing to prevent attacks is far easier than managing and responding to incidents, breaches, or a significant loss of systems or data.

OUR SCHOOL OR DISTRICT:

- [ ] Has conducted a security audit in the past 6 months; a third-party audit gives you a holistic view of how your technology is laid out and how to take appropriate actions when needed
- [ ] Has documented plans for dealing with any situation; an example is using the PICERL process (Preparation, Identification, Containment, Eradication, Recovery, and Lessons) as a best practice to prepare for each step of any security risk
- [ ] Communicates how to report (and avoid) phishing attempts

0 /3 Number of Boxes Checked

LEARN MORE: What to Do in Response to a Cybersecurity Incident >

SEE YOUR RESULTS >

Tips for Dealing with Top Cyberthreats

Phishing attacks—Educate end users, run simulated phishing attacks for staff, leverage your existing systems, deploy multi-factor authentication

Ransomware attacks—Remove system administrative rights for staff who don't require rights to do their daily work, give high-value targets (payroll staff and IT administrators) two tiers of access, patch systems regularly, analyze your network infrastructure, perform backup and recovery of your critical systems, create an education and response plan

IoT (internet of things) risks—Change default users and passwords, maintain an updated inventory of network devices, connect only the devices that need to be connected, review all IoT products before purchasing, use network segmentation, develop and implement a process for firmware updates, create BYOD policies

Student-driven attacks—Set clear expectations and model responsible behaviors, develop clear response processes for attacks involving students, protect against DDoS attacks, leverage cloud services for critical applications, use your existing systems for protections to monitor activity on your web filters, block access to known hack purchasing resources from inside the district

Reporting Phishing Attacks

Provide staff, students, and parents with an email address to forward all suspected phishing attacks. Your team can evaluate the emails and post a list and description of known attacks for others to see if they've received similar emails.

What's your cybersecurity score?

How many boxes did you check? 0

Look at the areas with lower scores to determine where to prioritize your next steps.

9 or less:

It's time for a cybersecurity overhaul.

Your edtech ecosystem and processes look to be vulnerable, especially when working remotely.

10-15:

We suggest you look at improving your cybersecurity practices.

You could benefit from a more secure system with clear training and procedures to ensure a safe environment.

16-21:

You're on the right path, but there's some room for improvement.

While you've made many safe decisions in how you're protecting data and ensuring cybersecurity, there are still steps you can take to help protect your school or district even more.

22:

Congratulations! You're a model of excellent cybersecurity.

You're an excellent custodian of student data placing a high priority on cybersecurity.

Improve Your Cybersecurity Readiness for Back to School

Schedule a customized demo to help meet your virtual readiness needs.

Visit www.PowerSchool.com or call 1-877-873-1550

PowerSchool

PS-PS-fl-002-072220