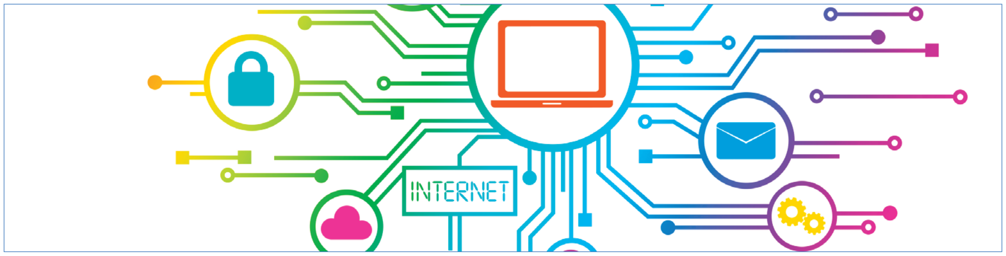
Electronic School



Security Goes High-Tech

Technology offers solutions to security dilemmas

TECHNOLOGY AND SECURITY ARE inextricably linked in K-12 schools. From dealing with crisis situations to safeguarding student and staff data, how you use the tools at your disposal is critical.

Choosing which tools to use also can be tricky. While the race to innovate shows no signs of slowing, especially in the cloud computing, data security, and app arenas, many school districts don't have the necessary funding or infrastructure in place to support the latest and greatest technology.

Thankfully, chances are that you can find the right solutions as long as you have a plan, a properly trained staff, and a vendor/partner who understands the nature of your district's security and data needs. And a little insurance doesn't hurt, either.

BUILDING SAFETY

Over the past two decades, schools have taken various steps to make their buildings more secure should a crisis arise. Security cameras are commonplace, but they are only one (increasingly small) piece of the puzzle.

Depending on the level of sophistication you want (and can afford), here are some tools you can and should consider.

- **Door access control systems:** Using security cameras and locked (from the outside) doors, your front office staff can verify visitors before allowing them into your school.
- **Digital signage:** With the cost of high-definition TVs dropping dramatically, it makes sense to put displays in your classrooms and hallways. Run through a central communications console, digital signage can be used for general information sharing and to alert students and staff in the event of an emergency.
- **Notification lights:** Part of a central communications console, these lights are installed in hallways, the cafeteria, auditorium, and gym and are used when weather or another type of emergency occurs.
- **Microphones and panic-call buttons:** Depending on how intricate your system is, these two tools also can be useful in crisis situations to alert students and administrators in the school.

Finally, many school districts require staff to wear identification cards and badges, and it's something you should consider for students as well. The technology we can put on a dime-size chip has become so sophisticated that the cards can be used for a variety of purposes—accessing buildings, buying food in the cafeteria, checking out books from the library—through a swipe, barcode scan, or chip reader.

The data you can collect from the use of these cards also can help you track what's working, what's not, and (most important) what is happening on your campuses.

Going one step further, technology known as "near field communication" is now available that allows students and staff to use a smartphone for this purpose, saving you the cost of buying and printing smart cards. Obviously, not all students have smartphones, so this won't work in every case, but it is something worth looking into down the line.

DATA SECURITY

Even though paper record keeping has not been completely eliminated, chances are that you have more than one of the following housed on a server or network: addresses, dates of birth, Social Security numbers, school ID numbers, test scores, free and reduced-price lunch forms, attendance records, medical forms, and payroll information.

What are you doing to protect this data? Not enough, it seems.

More than half of school districts do not have a full-time IT person on staff, according to a 2015 report by the U.S. Department of Education, and states have been slow to develop data security guidelines in the K-12 arena. This comes as districts look for ways to give students and parents more access to information online while managing to comply with the Family Educational Rights and Privacy Act (FERPA) and the Children's Internet Protection Act (CIPA).

Add to that the number of hackers who want access to your information and it's no surprise that schools and districts are vulnerable to cyberattacks.

ONLINE EXTRA
For more information and articles on school technology, go to **asbj.com/topicsarchive/technologyfocus**.

Fortunately, there have been several developments in recent months that can provide you with some guidance.

In Missouri, state auditor Nicole Galloway looked at the cybersecurity practices in five randomly selected school districts and found a number of "areas of concern." According to Galloway, schools should have a written data governance plan with steps that will be taken in case a breach or cyberattack occurs. Without a dedicated IT administrator, staff development on data security, and procedures for preventing simultaneous log-ins and password changes, districts will remain easy prey for hackers.

Another of Galloway's recommendations—developing procedures for monitoring a district's tech vendors—is addressed in a new initiative launched earlier this year by Common Sense Education. Working with 40 districts across the U.S., the nonprofit (www.graphite.org) has developed a series of guidelines that can help you test and evaluate a vendor's security and privacy practices.

In May, the Consortium for School Networking (CoSN) released a new tool, known as the Trusted Learning Environment (TLE) Seal Program, which can help districts ensure that digital data remains private and secure. According to CEO Keith Krueger, the program "gives schools the opportunity to build a culture of trust and transparency while harnessing the full potential of education technology."

POLICY AND PRACTICE

"Be prepared" is not just the Boy Scout motto. It's also a good rule to live by when you consider the vulnerabilities you face in the tech security arena.

Online security breaches have become so commonplace that school districts also should consider getting an insurance policy ito guard against attacks. Cyber insurance policies, which are an add-on to existing general liability and property insurance, are designed to protect you in case data such as Social Security numbers, addresses, and payroll information is stolen by hackers.

The Georgia School Boards Association has offered its districts a group cyber insurance plan since 2013 at a cost of about $1 per student. Two-thirds of the association's 95 districts have opted into the plan, which covers notification and investigation costs as well as legal and media relations assistance after a cyberattack occurs. Most important, the districts are covered if a related lawsuit is filed.

This type of policy should be a no-brainer for school districts, but again, resources play a role. Still, as you work to improve your own data security, you should shop around. Contact your state school boards association and see how it can help. Talk to local vendors. Consider becoming part of the TLE Seal program.

Take the necessary steps to be prepared, now rather than later.

Glenn Cook

Glenn Cook (glenncook117@gmail.com) is a Northern Virginia-based freelance writer and photographer, and former executive editor of American School Board Journal.

About the TLE Seal

To earn CoSN's Trusted Learning Environment (TLE) Seal, which was developed with input from leaders from 28 districts as well as several education associations, districts must address five areas:

- **LEADERSHIP:** Manage and collaborate with various groups regarding the use and governance of student data to inform instruction.
- **CLASSROOM:** Implement educational procedures and processes to ensure transparency while advancing curricular goals.
- **DATA SECURITY:** Perform regular audits of data privacy and security practices and publicly detail these measures.
- **BUSINESS:** Establish acquisition vetting processes and contracts that, at a minimum, address your district's level of compliance with laws while supporting innovation.
- **PROFESSIONAL DEVELOPMENT:** Require staff to conduct privacy and security training and offer related resources to everyone in the community.

For more information, visit http://trustedlearning.org.