Marketplace Update

The constant quest for school safety

K-12 schools are erecting physical and digital barriers to protect students. Are they enough, or even effective? Here's the state of school safety today.

BY ROBERT LEROSE

Securing K-12 schools takes a multi-prong line of defense. The physical campus needs to be fortified against live, in-person attacks, while the school needs to shield its IT/network from cyberattacks, protect sensitive data and monitor threats against all three.

Statistics paint a disturbing picture.

A report by the K-12 Cybersecurity Resource Center found that there were 122 publicly disclosed cybersecurity incidents at K-12 schools in 2018. Most involved data breaches where bad actors—including students sometimes—obtained unauthorized access to private information.

In about the same timeframe, the nonprofit Educator's School Safety Network found that at least 3,380 threats and incidents of violence were reported in K-12 schools in the 2017-2018 academic year—up 62 percent from the previous year. Shooting threats led the list (38.8 percent), followed by generalized or unspecified threats of violence (35.8 percent) and bomb threats (22.5 percent).

There are no national standards for making schools safer, but plenty of debate. As of November 2019, the National Conference of State Legislatures found that 167 bills had been enacted and eight resolutions adopted. School safety measures are decided primarily on a local or state level, resulting in a patchwork of regulations. For example, the Education Commission of the States found that only around 30 states allow security personnel to possess weapons in school and only about 42 states are required by law to conduct safety drills. Two recent initiatives, however, could significantly impact all K-12 school districts.

Trends in school security

First, in the wake of the tragedy at Marjory Stoneman Douglas High School in Parkland, Florida, Congress passed the STOP School Violence Act, which authorized the use of $50 million annually "to help districts implement improvements to school safety infrastructure."

Then, in September 2019, a bipartisan group of lawmakers proposed the School Safety Clearinghouse Act for K-12 students. Managed by the Department of Homeland Security, it would be the first effort of its kind funded by the federal government. The database would let state and local authorities draw on the recommendations of first responders, mental health advocates and other experts to devise best practices and procedures for strengthening their schools. Under the act, districts would be free to decide for themselves which actions to take.

There is no shortage of options.

Perhaps the most controversial is allowing teachers to carry firearms in the classroom. Florida passed such a law in October and gun regulations in other states make various allowances for firearms. Not surprisingly, the measure is opposed by groups such as the American Federation of Teachers, the National Education Association and the National Association of School Resource Officers.

A less contentious strategy involves "hardening" schools—installing different types of deterrents to fortify school buildings and protect students against intruders or violent threats. The latest data available (2015-2016) found that the most common security measures include: monitored doors, formalized plans to handle an active shooter situation, security cameras, locked doors, an electronic school-wide notification system, inside-locking classroom doors, locker searches and metal detectors.

Threats are just as prevalent on the network side. Schools are attractive targets for cybercriminals due to the abundance of personally-identifiable information (PII) on students and staff. Schools often have sensitive data pertaining to research–another lucrative draw for cybercriminals.

According to the K-12 Cybersecurity Resource Center, cybersecurity incidents involving U.S. public schools primarily involve phishing attacks, breaches or hacks resulting in disclosure of personal data, ransomware attacks, and other cyber incidents that disrupt school and result in unauthorized disclosures.

Many breaches in education are a result of poor security practices and little or no attention to detail, according to the Verizon 2019 Data Breach Investigations Report. Experts urge schools to be more proactive in defending their sensitive data and school networks, because as learning becomes more digital, networks are more susceptible to cyber threats and attacks. Correcting human error is the first step to avoiding these breaches. School IT leaders should establish a baseline level of security around internet-facing assets like web servers, and they also should strive to understand what groups or cybercriminals are most likely to seek out the kind of data the school or district possesses.

Two case studies

Increasingly, schools are using a combination of both physical barriers and network/IT solutions to beef up security. For example:

1. As the only urban middle school in western North Carolina, **Asheville Middle School** serves 750 students and is located close to the city. "We have a lot of transient people coming in and out. Just like any relatively large city, there's homelessness and street traffic. We try to be really careful about that," says April Dockery, principal.

The school contains several layers of security. For example, all exterior doors are kept closed and locked at all times. Visitors can enter the building only through one door and need to be buzzed in and then checked at the main office. The school also has an extensive ring of digital cameras on the building's exterior and in select places inside, such as in the hallways, staircases, gymnasium and cafeteria, but not in classrooms.

Each classroom has a direct phone to the front office so teachers can report problems. Dockery also has the option to bypass the PA system to send text messages to teachers and staff through Blackboard, an integrated communications system for schools.

According to the K-12 Cybersecurity Resource Center, cybersecurity incidents involving U.S. public schools primarily involve phishing attacks, breaches or hacks resulting in disclosure of personal data, ransomware attacks, and other cyber incidents that disrupt school and result in unauthorized disclosures.

Each grade is assigned its own color coordinated staircase so that school personnel can monitor student movement. Dockery and her team meet monthly to review and modify procedures and students are regularly drilled on safety behaviors, such as keeping quiet during fire drills.

2. According to Lori Jones, the assistant superintendent of technology services at **Northside Independent School District** in San Antonio, Texas, their schools follow the same type of security best practices that businesses do to secure their networks, such as having firewalls, multiple authentication checks, regularly updated passwords and switch port security, which protects the district's computer network from being hijacked by unauthorized parties.

The district also has a robust Internet filtering system to keep harmful content away from minors, complying with the Children's Internet Protection Act. "We try to secure the network while making sure we're providing a network that is available and usable to our user community. It's definitely a tradeoff on a daily basis," Jones says.

When an anonymous threat comes in, Northside schools will notify the local police and supply them with any leads, such as where the email came from and any IP addresses used.

The district is in the process of installing security lobbies at all its campuses. Northside staff members can use their badges to enter the building. Anyone without a badge must pass through a secure vestibule, provide proper ID and get checked through the school's security system before they can be buzzed in. Digital cameras scan outside and inside school campuses.

Not everyone is convinced that these measures will suffice. A recent paper from researchers at the University of Toledo and Ball State University concluded that "hardening of schools seems to be a questionable endeavor for most schools, given the dearth of evidence regarding effectiveness." The authors argue that schools should also have more mental health services, intervene earlier in episodes of bullying and teach conflict resolution to help stem violent behavior.

In the debate between aggression and deterrence, it seems that the conflict is far from over.

Robert Lerose is a freelance writer who covers issues and topics in the education sector.