—iStock/Getty Images Plus

Online Student Safety

EDITOR'S NOTE

The number of attacks on schools' networks and viral classrooms have seen significant increases. In this Spotlight, assess possible digital vulnerabilities; learn how students may be partaking in digital self-harm; gain insights on popular platforms; evaluate whether students are being groomed to accept over-surveillance; and consider the safety of students' data storage.

OPINION

—iStock/Getty Images Plus

Published on March 10, 2021

Cyberattacks on Schools Soared During the Pandemic

By Alyson Klein

Cyberattacks on school districts surged by a whopping 18 percent in calendar year 2020, likely due to the greater reliance on classroom technology during the pandemic, according to a report released March 10, 2021 by the K12 Security Information Exchange and the K-12 Cybersecurity Resource Center.

There were 408 publicly disclosed cyberattacks last calendar year, compared with 348 in 2019, the report found. That amounts to more than two attacks per school day. It's also the highest number of attacks since the Center first began tracking these incidents in 2016.

The pandemic "offered a profound stress test of the resiliency and security of the K-12 educational technology ecosystem," the report concluded. "The evidence suggests that in rapidly shifting to remote learning school districts not only exposed themselves to greater cybersecurity risks but were also less able to mitigate the impact of the cyber incidents they experienced."

School districts should review their plans for keeping tech operations running smoothly during future emergencies, the report suggested.

> "The evidence suggests that in rapidly shifting to remote learning school districts not only exposed themselves to greater cybersecurity risks but were also less able to mitigate the impact of the cyber incidents they experienced."
>
> **K12 SECURITY INFORMATION EXCHANGE AND THE K-12 CYBERSECURITY RESOURCE CENTER**
> MARCH 10, 2021 REPORT

In addition to the usual cyberattacks—denial of service, ransomware, phishing, and data breaches—the past year saw the introduction of a brand-new type of cyberattack: Invasions. 'Class invasions,' also known as 'Zoom raids' or 'Zoom bombing,' included unauthorized people disrupting online classes, often with hate speech, sexual or shocking images, videos, or threats.

So-called 'meeting invasions' used similar tactics and were targeted mostly at PTA meetings, school board meetings, virtual open houses, and other events drawing relatively larger groups of people. And 'email invasions' typically entailed breaking into district email servers and using them to send hate speech, distressing images, and other inappropriate content to many people on district email lists.

The pandemic may be a big part of the reason for the spike in cyberattacks, the report says. That's because schools increased their use of technology dramatically beginning last spring, including by handing out thousands of new devices, using new platforms without a lot of training for teachers, and allowing educators to use free apps that hadn't been carefully scrutinized for privacy and security factors.

What's more, school district IT staff may have used new remote access tools to keep teachers and students connected, creating more opportunities for hackers to get into their district networks. And, in districts where students returned in the fall of 2020 for some in-person instruction, many students and teachers brought back devices that were used on home networks that were not necessarily secure. That could have paved the way for malware— software specifically designed to disrupt, damage, or gain unauthorized access to a computer system—to enter district networks.

What kind of schools are most likely to be attacked? Traditional public schools lead the pack. And 12 percent of schools that were attacked once in 2020 experienced a second attack at another point in the year.

The report also found that urban districts are more likely to be attacked than small, rural ones. City districts make up just 6 percent of all districts, but were the target of 21 percent of the cyberattacks.

Meanwhile, large districts, defined as those with more than 10,000 students, comprise just 8 percent of districts, but experienced 31 percent of the attacks.

What should be done about cyberattacks?

For one thing, school districts should carefully examine the security practices of their vendors before they sign long-term contracts, the report recommends. Schools will need greater resources for cybersecurity if they are going to implement federal guidance on how best to safeguard their schools. And it's important for educators and students to understand basic cybersecurity measures, the report notes. ■

No computer lab? No problem with application streaming

In Anaheim, Amazon's AppStream 2.0 eases remote access to the Adobe Creative Cloud and could redefine how students use high-end software.

A transition to remote learning for schools in Anaheim, California, during COVID-19 posed a special challenge for high school students who take courses in computer labs. Without access to the specialized workstations in those classrooms, many students would be unable to use Adobe Photoshop, Adobe Premiere Pro, or other programs that were central to their courses.

To provide remote access to this software, the Anaheim Union High School District (UHSD) implemented Amazon AppStream 2.0, a desktop as a service platform from Amazon Web Services (AWS). The solution not only solved the problem of accessing software during COVID-19 but also sparked a discussion on better ways to deliver resource-hungry applications in the future.

Remote learning: A driver and a catalyst

Anaheim UHSD offers courses that use software from the Adobe Creative Cloud in approximately 38 computer labs spread across 19 buildings — eight comprehensive high schools, eight comprehensive junior high schools, an alternative high school, a virtual school, and a school that includes grades seven through 12. When the pandemic closed those buildings in spring 2020, these labs and their high-capacity computers were off limits to students.

The district managed as best it could. Some teachers directed students to alternative applications they could access from home via web browsers.

"They didn't have nearly the same feature sets as the Adobe products, but the teachers adapted the curriculum to use those other tools," says Erik Greenwood, chief technology officer (CTO) for Anaheim UHSD.

The district also converted its license with Adobe from a hybrid device and name-based structure to an entirely name-based model so students could access the Adobe Cloud from alternative devices. Some of the students covered by those licenses had enough computing power at home to log in and start working.

"Students who didn't have access to adequate technology to run the Adobe products at home checked out laptops in lieu of the Chromebooks we gave other students to enable remote learning," Greenwood says.

Greenwood's IT team also explored solutions like virtual desktop infrastructure (VDI) and application streaming.

"Remote learning was a driver and a catalyst," Greenwood says. "We had to come up with a solution to provide access to these applications remotely."

But while meeting the emergency need, an alternative approach might also solve another issue: how to give all students the same high-quality experience when they use the Adobe applications.

Like any computer hardware, Anaheim's computer labs need to be refreshed every few years. The district upgrades workstations as its budget allows, but it is not possible to replace them all simultaneously throughout the district.

"You have the challenge of different labs that have different technical specifications, with different levels of resources," Greenwood says.

A student assigned to a room with the latest machines enjoys a great experience. A student assigned to a lab with older computers may struggle with slower performance.

"We talked with our business teachers about VDI or app streaming as a possible way to provide a lower-cost device and have a consistent experience for students across the board, regardless of what classroom they happen to get scheduled into," he says.

A cost-effective and simple solution

Anaheim's IT department won support for the project by including key business teachers early in the conversation.

"We talked about the short, medium, and long-term potential of a technology like this," Greenwood says. "We seemed to

have buy-in from teachers we collaborated with for this to be a potential way of delivering the technology. Some of the teachers have been very willing to participate in the testing."

After evaluating several solutions, Anaheim UHSD's IT team chose AppStream 2.0. "Among the solutions we looked at, AppStream 2.0 had the best pricing, and it was full cloud," Greenwood says.

As an application streaming service, AppStream 2.0 is less expensive to implement than traditional VDI solutions and easier to manage. Instead of duplicating the entire desktop of a machine, AppStream 2.0 provides access directly to an application. From the Anaheim School District's landing page, the student clicks on an icon for the application and gets to work.

The Anaheim district implemented AppStream 2.0 in December 2020, working with InterVision, an AWS Premier Consulting Partner.

"There was a lot of iteration with InterVision, our teachers, and the IT department, setting up the images," Greenwood says. "And then a lot more iteration in spinning up those images, getting our teachers and students to try them and give us feedback, and then tweaking things as we identified them."

The bulk of the work took just a few weeks. "Then it was continual conversation about what fine-tuning we needed," he says.

Implementing AppStream 2.0 required very little upfront capital costs. The IT department is still determining the cost of ongoing operations, but the key is to analyze usage, which will be less predictable when students use the Adobe software from home rather than on campus during school hours.

"It's going to be a matter of fine-tuning the patterns of use to have the right resources within AppStream 2.0 available in a timely manner for students and teachers to be able to consume it," he says. "We are still figuring that out."

Digital equity and greater flexibility

Since December, the most obvious benefit of AppStream 2.0 is that students can use the Adobe applications remotely, regardless of whether they have access to powerful computers.

Based on how well it works for students and teachers, once schools return to 100 percent in-class instruction, the district will determine whether to continue using AppStream 2.0 to gain other, longer-term benefits.

For instance, the technology could let the district give all students who use the Adobe applications the same high-quality experience, which would provide a new level of digital equity.

"You will get the same access to computing power regardless of which classroom you are scheduled into," Greenwood says.

By eliminating the need to work in official computer labs, application streaming could also give students greater flexibility.

"A student could go to the library and fire up AppStream 2.0 on one of the general-purpose computers there or use his or her own device at lunch or on break," Greenwood says.

It also offers a potential financial benefit. "If it works as well as a hardware lab, we might not need a hardware lab," he says.

Anaheim is considering adopting a take-home computing model, in which the school district gives students a computer as needed.

"If I'm a student who takes video production, and the district is in a take-home environment, AppStream 2.0 could give me access to the tools I need on the device the district provides," he says. "And that might or might not necessitate a computer lab as we know it."

Whether enabling learning from home or enhancing instruction over the long term, AppStream 2.0 could expand options for students and teachers who use Adobe software and, potentially, software for engineering and related functions. "It definitely will provide more access to those applications," Greenwood says, "whether that's at school or at home."

This piece was developed and written by the Center for Digital Education Content Studio, with information and input from AWS.

PRODUCED BY: CENTER FOR DIGITAL EDUCATION

The Center for Digital Education is a national research and advisory institute specializing in K-12 and higher education technology trends, policy and funding. The Center provides education and industry leaders with decision support and actionable insight to help effectively incorporate new technologies in the 21st century. **www.centerdigitaled.com**

FOR: aws

Amazon Web Services (AWS) Worldwide Public Sector helps government, education, and nonprofit customers deploy cloud services to reduce costs, drive efficiencies, and increase innovation. Health and Human Services (HHS) agencies across all levels of government are leveraging AWS for initiatives ranging from the optimization of everyday administrative tasks to delivering a more personalized digital experience for citizens. Whether your focus is on agency modernization, helping to build healthier communities, or transforming payment and care delivery models, AWS has dedicated teams to help you pave the way for innovation and, ultimately, make the world a better place through technology. **Contact us** to learn how AWS can help you with your biggest IT challenges.

Published on February 16, 2021

What Educators Should Know About Digital Self-Harm During Hybrid and Remote Learning

By Mark Lieberman

As educators continue to plow through the challenges of keeping school going during a pandemic that has lasted over a year, they should be looking out for signs of students engaging in digital self-harm, researchers say.

A recently published study led by a Florida International University researcher found that 1 in 10 students in the state said in a 2019 survey that they had cyberbullied themselves in the past year. Research on this specific type of cyberbullying remains thin, but efforts are underway to expand understanding of the issue.

Justin Patchin, professor of criminal justice at the University of Wisconsin-Eau Claire and co-director of the Cyberbullying Research Center, believes educators should know more about digital self-harm so they can be on alert for it and perhaps even help contribute to broader understanding of how it works and how it might be prevented.

Education Week asked Patchin to explain what we know so far about digital self-harm, and how educators should address it during a period when much more schooling than usual is happening online.

The following telephone interview was edited for length and clarity.

—iStock/Getty

What does this phenomenon look like?

It can happen on any platform. The earliest examples that we saw were on anonymous social media apps like Ask.Fm that encourage you to be anonymous, and don't require you to be your real identity. The way the platform works is you have a profile, anonymous people ask you questions, when you reply they show up only in your feed. You could ask yourself why are you so stupid, why are you so ugly, etc. To be sure, somebody could set up a fake Instagram profile or fake Snapchat profile and use it to target somebody else or use it themselves. It's basically when somebody anonymously makes hurtful comments or threats towards themselves in a public venue so that others can see it.

How did you first learn about this problem?

We became interested in this problem five or six years ago when we had heard a couple of examples of situations like this. In one high-profile situation, a 14-year-old girl in England had killed herself. One of the causes of that suicide was cyberbullying that had happened on a particular social media platform. When the authorities investigated, most of the hurtful messages that were being sent to her originated from her own computer, from her own bedroom. She had sent the messages to herself.

We had been studying cyberbullying among adolescents for probably a decade at that point, and we hadn't considered that students would send hurtful messages for themselves. We looked around [to see] if anybody had done any research on it. There were a couple of blog posts speculating, but that was about it, so we decided to do it ourselves. We figured it would be a pretty rare phenomenon.

In 2016, we surveyed 5,500 12 to17-year-olds across the U.S., and included a couple of questions in that survey about if students had posted something hurtful about themselves online. To our surprise, we found the numbers were higher than we expected. Five or 6 percent of kids had done this. Boys were slightly more likely to do it than girls.

Among the kids who had done it, we asked them to tell us why they did. Most of the reasons given were what you'd expect: for attention, to see if anybody would help them, to see if anybody would do anything about it. Some said they did it because they were bored, or to be funny. More boys said [they did out of boredom or to be funny] than girls, which might explain the sex difference there. We replicated that [study] in 2019 and essentially found some of the same things, but we haven't had a chance to publish those data.

What causes kids to engage in this kind of behavior?

We know some of the variables that are correlated, but we don't know if x causes y. We know kids who participated in digital self-harm were significantly more likely to also have depressive symptoms, also participate in physical self-harm, also to have attempted suicide. We don't know which came first. This is the ultimate question. Do kids get de-

pressed, and then they post negative things online, or physically hurt themselves? Is it part of a constellation of things that happen at roughly the same time? There's definitely a lot we still don't know about those behaviors.

What effect might the pandemic be having on this behavior?

We're trying to collect data in the next couple months, and hopefully we can include some of these questions. We know that kids are online more. Potentially that creates more opportunities for them. The other concern about remote learning, we've heard examples where students haven't had access to resources at school such as school counselors or psychologists or school social workers. If a child is dealing with some issues, they are depressed, maybe they don't have somebody that they can talk to because of remote learning. Therefore it might be a lot more difficult for them.

We study cyberbullying more broadly, and there's a lot of speculation now about whether cyberbullying has increased. There's no clear data, but there are some people that have reported seeing more reports of cyberbullying. We did see a little bit of an uptick early on, especially as particularly young kids were given access to technology they maybe didn't have before. On the other hand, we know from our research over the last decade that most adolescent cyberbullying is connected to school relationships or even school bullying. If kids aren't at school they're not having those disagreements. We've had kids who have said remote learning is better for them because they don't have to deal with bullies at school.

What can be done to prevent digital self-harm?

It is hard for a teacher or a parent to get to the bottom of this. From the standpoint of their role whether as an educator or a parent, if they learn about a child being cyberbullied, they need to investigate. They need to talk to the kids involved, report it to the website or app. If it is particularly bad, egregious, if there are threats of physical harm, it will be flagged by these apps. The apps can identify this pretty easily. Whether they'll share that with you is a different question. They'll share it with law enforcement, which is unfortunately where we often find out about these things, if there's a pretty serious incident.

What we've found is, it doesn't really matter who is doing the cyberbullying. You need to provide resources to who's experiencing it. Whether you're doing it to yourself or someone else is doing it to you, our goal should be to help you. That might be very practical things like showing you how to block a person from your account, collect evidence, report it to the apps. But maybe it is a cry for help or you do need some kind of counseling or other assistance.

Schools should open up an opportunity for students to report to them if they're being mistreated in a way that affects the school environment. Whether having some online reporting mechanisms or a particular person that people can turn to, but then hopefully having some resources in the school whether through a counseling department or school psychologist who's trained in online abuse behaviors. ■

Published on July 29, 2020

What Educators Really Need to Know About TikTok

By Benjamin Herold

Is TikTok really mining mountains of data from children, giving the information to the Chinese government, engaging in political censorship, and leaving its users vulnerable to hacking?

All four issues have been in the headlines recently. Here are answers to the questions teachers, administrators, and policymakers are likely to have:

First, let's take a look at how educators are using TikTok.

Uber-popular with tweens and teens, TikTok is a video-sharing platform on which users share short (60-seconds or less) clips of dance moves, comedy, memes, art, viral challenges, and just about anything else you can imagine. To wit: Ed Week's "principals of TikTok," who use the platform for everything from demonstrating proper COVID-19 cleaning protocols to sharing absurd moments from the school day. Many teachers also turned to TikTok spring of

2020 to entertain their students and vent about remote learning.

The app has been downloaded more than 2 billion times worldwide, with well over 120 million active users estimated in the U.S. alone. That translated to an estimated $17 billion in revenue in 2019.

What's the biggest thing I need to know right now?

That would be the renewed privacy concerns.

Like many other social-media platforms, TikTok collects gobs of information from users, including the contents of their private messages, what type of device they're using, their internet protocol (IP) addresses, and all manner of information on what types of videos they watch and how they watch them. Under its loosest settings, TikTok can also collect from users' age, phone number, precise geolocation data, and more.

While this is a general concern for all users, many privacy advocates are particularly concerned because of TikTok's huge adoption by tweens and teens.

This spring, the Campaign for a Commercial-Free Childhood and a host of other organizations (including Consumer Reports and the Parent Coalition for Student Privacy) filed a complaint with the Federal Trade Commission. Among the groups' allegations: that TikTok fails to obtain "verifiable parental consent" before collecting information from children under 13; fails to offer parents the right to review and delete young children's personal information; and doesn't offer a clearly labeled link to its online privacy notice.

"Strong FTC action is needed to protect children from substantial risks to their privacy and well-being that come from sharing some of

the personal forms of personal information—their images, their words, and their thoughts—to TikTok's 800 million users worldwide without their parents' knowledge and informed consent," reads the 56-page complaint.

This sounds familiar...

That's probably because TikTok's predecessor company, Musical.ly, settled with the FTC in 2019 for failing to post a clear privacy policy, failing to provide direct notice to parents, failing to obtain verifiable parental consent, and failing to delete children's personal information at the request of parents.

The $5.7 million settlement did not include an admission of guilt, but the company did enter into a consent decree in which it vowed to no longer violate the Children's Online Privacy and Protection Act, commonly known as COPPA. The new complaint alleges that despite the company's new registration process, updated privacy policy, and the deletion of summer user information, TikTok is "continuing to flout" that agreement.

The company has also been hit with a number of private class-action lawsuits related to COPPA violations, including one by Illinois parents that it recently settled for $1.1 million.

Remind me what COPPA is all about?

In short, the federal law requires companies that offer websites, apps, and online services to notify parents and obtain their consent before collecting any personal information on children under 13.

Didn't TikTok add a new, more limited account for children under 13?

Yes.

According to a December blog post by the company, "TikTok for Younger Users," as the service is called, "introduces additional safety and private protections" including a view-only mode and "extensive limits on content and user interaction." The company also recently launched a Youth Portal, to teach about internet safety, and new settings to give parents more control over how their children use the platform.

However, the Campaign for a Commercial-Free Childhood and its fellow complainants allege that the age gate that's supposed to direct pre-teens into these "younger user" accounts is ridiculously easy to bypass.

They also allege that TikTok is still collecting and sharing prohibited personal information from even these younger-user accounts.

Sounds like a problem for the company and for parents. Why do educators need to worry about this?

First and foremost, large numbers of your students are almost certainly on TikTok. At minimum, you need to know what the platform is and how kids are using it–including for viral challenges that have sparked fires and electrocution concerns in schools, as well as racist and offensive content that administrators are often left to deal with.

Despite the classroom management challenges it can pose, some schools have also started experimenting with the platform as an instructional tool and as the basis for school clubs.

And TikTok has been vocal about its intention to get into the education market, announcing earlier this year a $50 million Creative Learning Fund that "supports creators with the production of learning content, provides resources for learners, and introduces emerging teachers to the TikTok platform." As part of its #LearnOnTikTok effort, the company has enlisted prominent partners such as science educator Bill Nye and motivational speaker Tyra Banks to produce educational content.

What does the company say about these privacy concerns?

"TikTok takes the issue of safety seriously for all our users, and we continue to further strengthen our safeguards and introduce new measures to protect young people on the app," a company spokesperson said in a statement. "We are committed to continuously evaluating and improving our protections.

In a series of recent statements, the company has also responded to a wave of security-related concerns, including reports that users were vulnerable to hackers and that the platform accessed iOS users' sometimes-sensitive clipboard content.

How is this related to the former Trump administration's threats to ban TikTok?

In recent weeks, both former President Donald Trump and former Secretary of State Mike Pompeo have raised concerns about TikTok's Chinese ownership and relationship with the Chinese Communist Party. Central to their complaints are worries that the company might currently, or could be compelled to, share users' personal information with the Chinese government, which is in the midst of building one of the most extreme digital surveillance states on the planet.

Calling TikTok a "cyber threat," the U.S. Army has also banned the app (which it has used as a recruitment tool) on government-issued phones.

The administration and some U.S. lawmakers have also raised censorship concerns, worrying that the company may be changing or removing some videos to protect the political interests of the Chinese government (around Hong Kong's independence, for example.) In response, a government group called the Committee on Foreign Investment in the United States announced a national security review of the company in 2019.

For its part, TikTok has said that it stores all data from U.S. users in the United States and Singapore and that the information is not subject to Chinese law. There is no public evidence to date that Beijing has accessed TikTok users' information.

In addition, the company said in a June statement, "we have never been asked by the Chinese government to remove any content, and we would not do so if asked."

Is this a partisan flap?

No.

The former Trump administration's trade war with China has clearly brought fresh scrutiny to TikTok's parent company, ByteDance.

But a host of Democratic lawmakers have also raised concerns. In 2019, for example, Senate Minority Leader Chuck Schumer, a Democrat from New York, joined Republican colleague Tom Cotton of Arkansas in calling TikTok a "potential counterintelligence threat we cannot ignore."

And in May, more than a dozen House Democrats, led by Ann McLane Kuster (N.H.) and Jan Schakowsky (Ill.) submitted a letter to the FTC supporting the new privacy complaint against the company.

"Given the reasonable concerns that the Chinese government may have access to the data TikTok collects on Americans, it is all the more troubling that the company appears to intentionally be in violation of U.S. data privacy laws," the lawmakers wrote. ■

Additional Resource

For all the detail you could possibly want, here's the full EdWeek explainer on COPPA and Schools: The (Other) Federal Student Privacy Law, Explained.

—Getty

Published on August 11, 2020

School Reopenings Bring Wave Of COVID-19 Student-Data-Privacy Concerns

By Benjamin Herold

Whether it happens in-person or remote, in-person learning is bringing with it a host of new data privacy concerns.

Chief among them: How to safely and legally store and share videos of classroom lessons featuring students, and what to do with all the new sensitive health information being collected by schools now administering health surveys, doing daily temperature checks, and tracing the contacts of students and staff who have contracted or been exposed to the coronavirus.

"Reopening plans must balance protecting health and protecting student privacy and educational rights," said Amelia Vance, the director of youth and education privacy at the Future of Privacy Forum, which earlier this month released a new "Student Privacy and Virtual Learning Guide" along with the National Center on Learning Disabilities.

"It is a difficult—but incredibly important—balance," Vance said. "Schools and districts should have clear plans in place for how they will collect, use, and store health data to ensure it is not ultimately used to limit educational access or opportunities for vulnerable students."

Remote Learning Drives Ed-Tech Expansion

With the coronavirus pandemic still ravaging the country and sowing uncertainty in schools, 9 in 10 district leaders say they plan to incorporate some level of remote instruction into their reopening plans, according to the most recent survey of K-12 professionals administered by the Education Week Research Center in late July of 2020.

That means an abundance of platforms, software programs, and apps will be a regular part of students' education. With this new reality comes fresh concerns about how all that technology will be collecting, storing, and using students' personal information. Parents who wish to opt out of such technology usage, already limited in their options before the pandemic, will now be even more constrained.

To minimize the potential risk and build trust, Vance said, schools should consider establishing and sharing a set of limited and vetted ed-tech products they intend to use during remote learning.

That list shouldn't include social media. Despite the appeal of reaching students on the platforms they regularly use in their personal lives, teachers and administrators should avoid delivering instruction on platforms such as Instagram Live, TikTok, and YouTube.

"Many social media tools were developed for general audiences, not students, and are therefore unlikely to be compliant with student privacy laws and best practices," according to a blog post from the Future of Privacy Forum this spring.

And what about providing teletherapy services to students with special needs or disabilities?

Avoid "public-facing" platforms like Facebook Live, the new virtual learning guide advises, and, if possible, use platforms that your school district has a contract with. The federal department of Health and Human Services has offered greater flexibility around using commercial services that are not public-facing, such as Zoom, Facebook Messenger, and FaceTime.

Tips for Data Safe Videoconferencing

How are schools managing the broader shift to video-based instruction?

Eighty-two percent of district leaders expect teachers to pre-record video lessons and make them available for students to watch on demand, according to the most recent Ed-Week Research Center survey. And when it comes to live videoconferencing, 8 in 10 principals and district leaders have approved their schools to use Zoom or Zoom for Education and Google Hangouts. Smaller numbers have approved use of Microsoft Teams, GoToMeeting, Skype, and other platforms.

A student's mere participation in such videoconferencing likely does not trigger the Family Educational Rights and Privacy Act, or FERPA, the nation's primary student data-privacy law. That likely changes, however, the moment "a student's image, name, or voice is recorded and stored by the school," according to the new NCLD and Future of Privacy Forum guide.

To make sure schools are protecting students' privacy during videoconferences, the Consortium for School Networking, a professional association for school-technology leaders, developed an online guide.

Whenever possible, avoid recording classroom discussions with students, the group advises. Create guidelines that ensure any videos involving students are secure both in transit and while being stored. Make sure only necessary personnel can access the videos and set a schedule for deleting all videos after a set period of time.

> Many social media tools were developed for general audiences, not students, and are therefore unlikely to be compliant with student privacy laws and best practices."
>
> **THE FUTURE OF PRIVACY FORUM**
> BLOG POST FROM SPRING 2020

Also critically important, said CoSN CEO Keith Krueger, is to avoid any "practices that might result in the videos being publicly available." That means no open Google Drive links, posts to private YouTube accounts, or emailed files.

One strategy used by many school districts trying to take such concerns into account: Using learning management systems that are specifically designed for K-12 schools and have built-in tools for meeting with students, such as Canvas.

Protecting Sensitive Health Data

Another new concern for schools is all the sensitive health data on students now being collected.

In late July of 2020, 3 in 5 district leaders told the EdWeek Research Center they planned to do daily temperature checks of students and staff. Ninety-two percent said they'd require sick students to stay home, and 79 percent said they'd require students who were exposed to the virus to do the same. A handful were also planning to administer their own COVID tests.

"The complexity of this work across students and employees can't be overstated," said Krueger of CoSN. "In addition to state reporting requirements and privacy laws, schools also need to consider anti-discrimination laws, labor laws, and more."

As important as ever, he advised, schools should avoid rushing a technology solution into place just to create the appearance of action. Strong privacy and security measures—including legal reviews for compliance with state and federal law, plans to minimize the data that are actually stored, limiting access to those data, and ensuring that "robust physical, technical, and administrative controls" are in place—are essential.

One tangible example of data minimization that Krueger described: A record stating that a given student will be attending classes remotely for two weeks is far less invasive, sensitive, and susceptible to misuse than a record indicating that student had a high temperature and exhibited other coronavirus symptoms and therefore is being forced into quarantine for two weeks.

Be careful of the proliferation of symptom-tracking apps now marketing themselves to schools, said Vance of the Future of Privacy Forum. Many have privacy policies that indicate compliance with HIPAA, the federal health-privacy law, but do not mention FERPA, which is the law most likely to actually apply to use in schools.

There are also important considerations around equity and anti-discrimination to consider, many of which are discussed in detail in a series of issue briefs created by the forum. Trust is essential, said Vance, so parents and students feel comfortable honestly reporting their symptoms, without worry that such information might be used to exclude them from certain classes or educational opportunities down the road.

To that end, experts across the board stressed a common point: In a time of high anxiety and tremendous uncertainty, as back-to-school season is certain to be, transparency is critical.

"If there was ever a time to over-communicate with parents about your [privacy] plans," Krueger said, "this is it." ■

Additional Resource

An unprecedented number of online interactions between teachers and students from their respective homes introduce new privacy questions that lack easy answers. See more EdWeek coverage on student privacy here: Massive Shift to Remote Learning Prompts Big Data Privacy Concerns.

—iStock/Getty Images Plus

Published on February 8, 2021

Cybersecurity Training for Educators Lagging Behind Rising Risk of Cyberattacks

By Alyson Klein

With almost 80 percent of K-12 and college-level educators reporting that they are using some sort of online learning platform during the pandemic, keeping virtual classrooms secure seems more important and difficult than ever.

But 44 percent of K-12 and college educators say they haven't received basic cybersecurity training, and another 8 percent were unsure if they had been trained at all. That's according to an October 2020 survey by Morning Consult on behalf of IBM, a technology company.

The survey also found that nearly half of K-12 and college educators–46 percent–aren't familiar with "Zoom-raiding" or "video bombing", which is when an outsider interrupts an online lesson, sometimes using racial slurs or sexually-charged language or images.

That finding is despite the fact that many educators teaching in full-time remote or hybrid learning environments have experienced the problem. Nearly a quarter of those surveyed–22 percent–say at least one of their colleagues has experienced some security-related issues during the pandemic.

What is especially problematic from a cybersecurity perspective is that more than half of K-12 educators, 54 percent, report using their own personal computing devices for remote learning. Such devices tend to lack the same

level of cybersecurity protections as school-issued computers.

What is also troubling is that more than a third of K-12 educators say their districts have not provided any guidelines or resources to help better protect the devices they are using for virtual teaching.

Schools are prime targets of cyberattack

Yet schools are among the institutions most likely to be targeted by hackers during this period of heightened attention on cybersecurity threats, Richard DeMillo, interim chair of the School of Cybersecurity and Privacy at the Georgia Institute of Technology, told Education Week in a November 2020 interview.

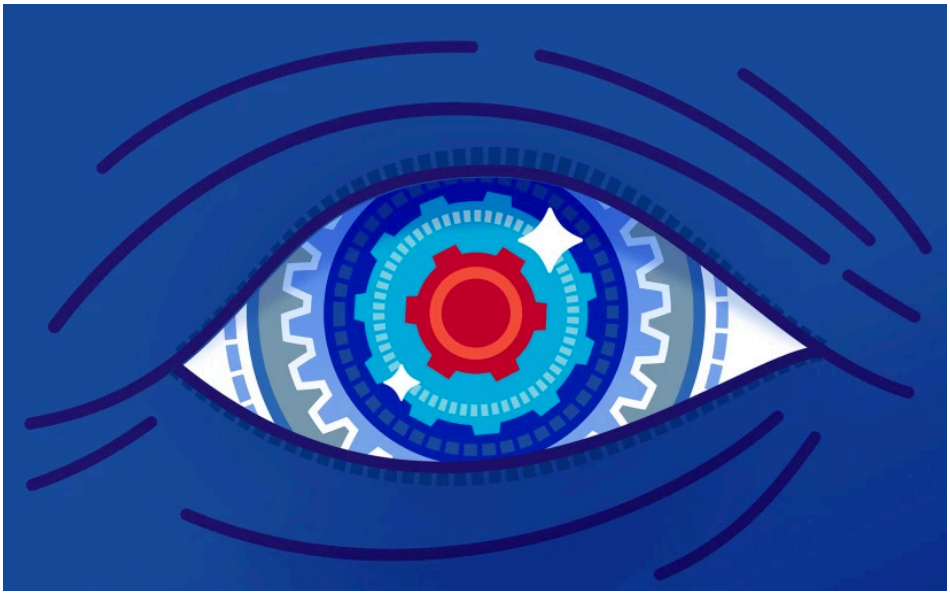
Public institutions that have a strong motivation to protect their data are always at a higher risk, and the pandemic has increased that risk because far more school activity is occurring using digital tools.

"It's not that the threats are changing, it's that the risks are growing," DeMillo said. "You should assume the more you're doing online, the more the risks have gone up, the more serious the consequences would be if there were a serious breach."

Overall, the IBM/Morning Consult survey found that about half of K-12 and college educators, 47 percent, are worried that their institution could be the victim of a cyberattack. Another 50 percent of educators say they aren't very concerned, or aren't concerned at all.

Educators are more likely to worry about external sources–such as cyber criminals– causing an attack than students. Fifty-seven percent of educators say they are "very" or "somewhat concerned" that cybercriminals could attack their institution or district, compared with 39 percent who felt the same about students.

The survey was conducted from Oct. 15 to 22 of 2020 and included 1,000 K-12 and college educators, plus 200 K-12 and post-secondary education administrators. It has a margin of error of 3 points for educators, and 7 points for administrators. ■



—Brandon Laufenberg/DigitalVision Vectors

Published on April 2, 2021

Teachers Are Watching Students' Screens During Remote Learning. Is That Invasion of Privacy?

By Stephen Sawchuk

At first, Ramsey Hootman thought something might be wrong with her son's school-issued laptop. All of a sudden, most of the browser tabs he'd opened had closed, seemingly of their own accord.

It took a little while to figure out that the culprit was actually a teacher, who'd used a tool called Securly Classroom to view her son's screen and close out all but two of his tabs—an action that, to both mother and son's frustration, gunked up an assignment he'd been trying to research.

Remote classroom-management tools like Securly Classroom and its competitors give teachers an expansive, real-time look into what their students are viewing or working on. As Hootman discovered, they also contain a panoply of features, like the ability to freeze a student's screen, or to call up, block, or limit tabs.

In interviews, some teachers said they use the tools in productive ways rather than to spy or punish, and that the tools have smoothed out some of the tough work of remote schooling. But the systems also raise questions about an ever-expanding surveillance apparatus in American schools.

"My main objection is the personal level of the surveillance. It's not generalized; it's not a 'ping' from some student who used some trigger word. His teachers are looking, in real time, at what he's doing," said Hootman, whose children attend school in the West Contra Costa, Calif., district.

The companies that sell the products say the tools help replicate good brick-and-mortar classroom practices. Just like circulating about a classroom, a teacher using them can ensure students are on task, and quickly assess who might need some additional, personalized help.

But one thing is abundantly clear: Use of remote classroom-management tools has undoubtedly increased over the last year as millions of students learned full-time from home.

Districts have scrambled to get millions of devices into the hands of students and to respond to the needs of their teachers, most of whom have never taught remotely before and are desperately seeking ways to engage students. And, noted privacy experts, the nation's experiment with remote learning has

blurred the line between home and school to an unprecedented degree.

"When you're at home, this monitoring starts to feel much more invasive and creepier. But it is going to continue long after students are no longer primarily at home," said Amelia Vance, the director of youth and education privacy at the nonprofit Forum on Privacy.

"So there's the need for clear information from schools that have installed these products, why they're installed, what the data protection is, and what the rights of students and parents are," she said. "It's something we rarely see in student privacy conversations."

How do remote classroom-management systems work?

The monitoring of students' web use is hardly new. Beginning with the federal Children's Internet Protection Act, in 2000, districts receiving federal school-connectivity funds had to install internet filters on their hardware and devices to protect children from obscene content.

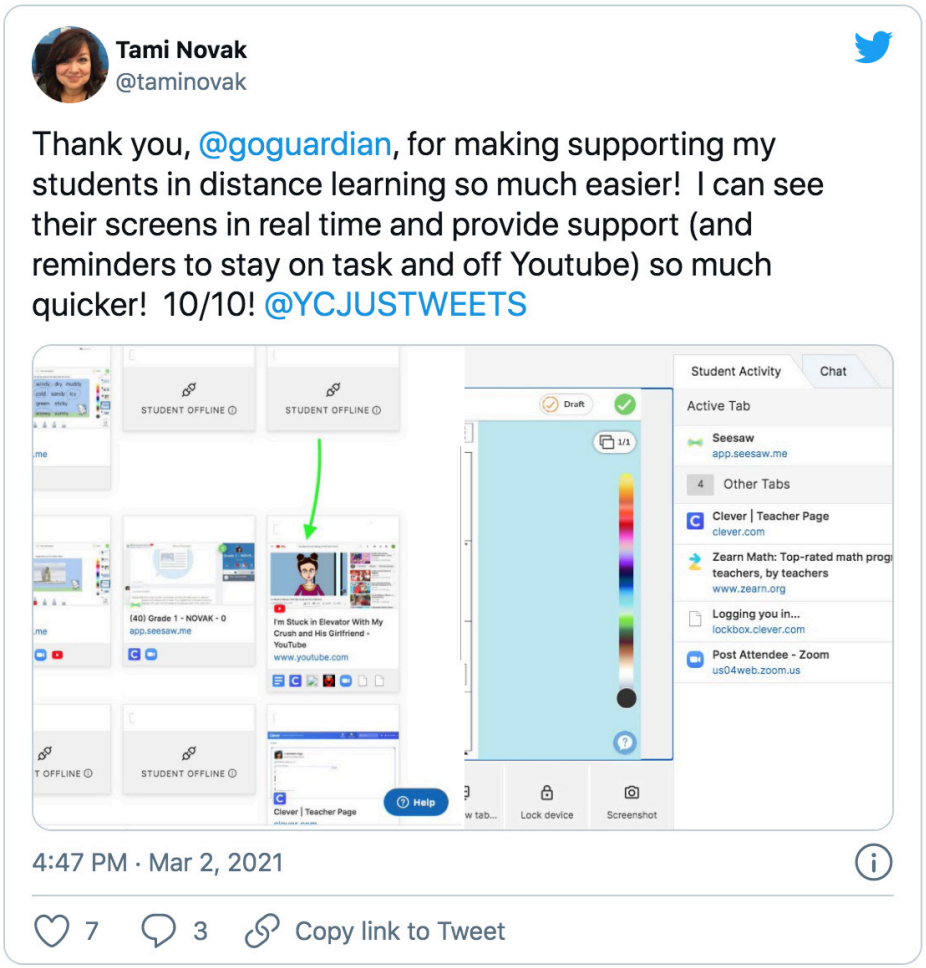
Actual thumbnail-like monitoring of individual devices also dates back decades. One provider of classroom-monitoring software, LanSchool, began in 1986, when all school computers were hardwired in labs.

The movement toward cloud computing and increased fears about student safety—coupled with ambiguities in the CIPA law, which did not detail where surveillance should stop—means that as the tools have evolved, they've grown more powerful.

Two of the top companies in the space, GoGuardian and Securly, both got their start by providing cloud filtering services to districts, but have since expanded to other products. Their remote classroom management offerings are respectively known as GoGuardian Teacher and Securly Classroom.

The remote classroom-management systems work like this: They are extensions to the Chrome browser that are deployed on students' district accounts.

Teachers activate a session at the beginning of a synchronous remote class. Then, they can see thumbnails of each student's screen, review the tabs they have open, and scan the web address of the websites they've visited. They can also freeze students' screens, restrict the number of tabs students have open, close tabs if students are on YouTube, Spotify, or other sites not related to the day's lessons, and push out links and messages to students. Students, for their part, can "raise their hands" virtually to request help.



The systems do alert students when a session is beginning. And an extension icon or indicator in the browser signals when their screens can be viewed.

While designed primarily for Chromebooks—by far the most common classroom device—they can be made to work on other hardware. And depending on how permissions are set, the services can also work when a student uses a personal device rather than a district one to access their school account, if the Chrome browser is set up to "sync" extensions.

Neither GoGuardian nor Securly's products permit districts to turn on device cameras remotely, or see into students' homes, officials at the companies underscored. (There have, however, been a few snafus stemming from how the services interact with other tech applications.)

Teachers say the tools enable efficient feedback to students

Among teachers who regularly use them, the tools appear to be broadly popular.

Kathy Richardson, a high school biology and marine ecology teacher, teaches in the Louisa County, Va., district and for a regional online learning collaborative. She's used GoGuardian Teacher for several years, and she believes the pandemic has actually helped refine her use of it.

Before, she said, she used it mostly to make sure students were on task. But now she uses it to pinpoint which students need coaching on tricky tasks like calculating a standard error for their lab reports.

"For me, the biggest aid in using it has been identifying where they're getting stuck, where these misconceptions and misunderstandings are," she said. "Before, I would go back and explain the whole section. Now I can get very specific about what's wrong; maybe it's a graphing issue, not a content issue."

She likes being able to pop into students' screens so she can suggest they change their y-axis or put their data into a bar graph. Sometimes, students ask her to view their screens so she can double check their work.

Most of all, she said, it has made instruction stronger during the pandemic.

"Even though the curriculum is a little slimmed-down, I think they're getting deeper in it than they would have otherwise," she said.

Enoch Kwok, the director of technology for the Oak Park district in California, believes most of the school district's teachers use it for similar purposes.

"I don't think a lot of our teachers are playing police and trying to catch kids out. If you make the lesson relevant and engaging enough, students will focus on that instead of goofing off," he said.

It is hard to say precisely how common the services are: They're often bundled with the companies' other security products. And like other privately held ed-tech firms, the companies don't share proprietary financial data. But both Securly and GoGuardian officials said that their tools have been popular.

The pandemic has accelerated interest in Securly Classroom, which the company launched in 2019 after acquiring its progenitor in a merger. Even before COVID-19 hit, though, the company was seeing tremendous growth in its sales, said Jarrett Volzer, the general manager of mobile device management and classroom technologies for Securly.

GoGuardian, which launched the Teacher service in 2015, offered it to districts for free in the spring of the 2019-20 school year, after the pandemic caused nearly every school in the country to shut down. About 20 million students and 14,000 schools now use a GoGuardian service of some kind, a spokesman for the organization said.

And according to a February survey of about 1,200 educators conducted by the EdWeek Research Center, more than two-thirds of respondents believe their districts will continue to offer remote learning options even after the pandemic ends.

Communicating with parents about monitoring tools is key

District technology officials have significant latitude to customize how the tools work and to constrain the hours when teachers can launch the live sessions, typically during regular school hours. They also tend to give teachers significant latitude on whether to use the remote classroom-management tools.

That's why the companies say they encourage districts to be purposeful in explaining to parents how they work.

"I would underscore and double click on the idea that while we provide the technology, schools use it to enact their policies," said Teddy Hartman, the head of privacy for GoGuardian. "A fair amount of the questions we get are parents who feel that the school system did not communicate well with them."

Communicating all those nuances is difficult, though, and probably also explains why some parents shrug at the use of the tools while others like Hootman, the California mom, feel caught out.

Hootman said that before the incident with Securly Classroom, she'd made her peace with some degree of school surveillance. She knew certain websites were blocked and that her sons' documents could be read by administrators. (One of her sons, in fact, once got flagged by the district's safety auditing service when he jokingly used the Klingon phrase "Today is a good day to die.")

But she was annoyed by how she found out about Securly Classroom.

"What really got me was that as soon as [the school] got [this tool], they escalated to the most restrictive possible environment. And they just really expected us to be glad about this," she said.

Tracey Logan, the district's technology director, said it added Classroom at the start of this semester, as teachers asked for more help with online learning. West Contra Costa doesn't mandate that teachers deploy the service; some educators like all its bells and whistles, and others use it minimally, she said.

In that district, Securly Classroom has been popular for teachers of very young students, English-language learners, and students with disabilities. In those classes, age, language barriers, or other issues mean getting everyone logged into and set up in a remote session is harder so the tool helps save valuable instructional time. Math teachers also like it.

But communicating about the tool in the 28,000-student district has fallen primarily to individual principals and classroom teachers. And Logan said she understands why parents might feel uncomfortable depending on how they learned about it.

"I can see how psychologically, they might think: Can they see through that webcam? Are they capturing keystrokes? I get how it can feel weird," she said. (The service does not do those things.)

In other districts, the problem has been

exacerbated when the programs deploy on families' personal devices.

Chris Carman, a high school science teacher in the Kent City, Ohio, district, only learned about the tool's reach only after he got an email from his son's science teacher, admonishing the 7th grader for working on a social studies assignment during class. (Carman's son had been using the family's own device, not the school system's.)

Being off-task is a legitimate concern for teachers to bring up, Carman agreed. But the message got diluted by how intrusive the notification felt. (The district, he said, sent an email about GoGuardian Teacher to parents shortly after Carman inquired whether his son could opt out of the sessions. The district's tech director did not immediately return an email seeking comment.)

"Frankly, I was just offended by the disregard of our privacy. I know the district, and others, see this as technically students are in school. But my son's not using their device, and he's not using their WiFi or Internet connection. That was what really bothered me," Carman said.

"It was the consent aspect of it; if they'd asked me beforehand, I would have had time to think about it," he continued. "Most importantly, I would have had time to talk to my son."

> "I'm realizing that with this generation—two if you count the millennials—not only do they not have this expectation of privacy, they don't even know what privacy means."
>
> **CHRIS CARMAN**
> HIGH SCHOOL SCIENCE TEACHER, KENT CITY, OHIO

Some students worry about monitoring, while others not so much

Just what do students whose daily school activities are being monitored by these programs make of it?

Some are predictably cross that they can't sneak off to play Fortnite or watch YouTube when they're supposed to be analyzing "Song of Solomon" or working on trigonometry ratios. But others have expressed bewilderment or anger, finding the surveillance intrusive or dystopian.

At a minimum, students are paying attention to the debate.

It was a high school newspaper, the Grizzly, that first reported Oak Park's pilot program allowing GoGuardian Teacher to stretch to families' personal devices.

"I think it's a little scary to know that my teachers can see what I'm doing. It would be more beneficial for teachers to find a less invasive way to limit cheating," the newspaper quoted one senior as saying.

J.P. Kerrane, a 15-year-old freshman in the Boulder Valley district in Colorado, says some students there definitely feel that someone's constantly "watching over their shoulder" when teachers use the classroom-management program. Many teachers in the district have chosen not to deploy GoGuardian Teacher for that reason even though they have access to it, he said.

Other students don't sweat it, he said—their reasoning roughly paralleling school district officials nationally who assert there's nothing to fear about monitoring if students are following the rules. Some of Kerrane's peers, in fact, have even made funny memes about GoGuardian—like one which depicts the horrified expression of a teacher perusing student-written fan fiction.

But personally, he's not so sure.

"I think I'm more privacy-conscious than most. I know everything I type into Google Docs is being sent to an algorithm to see if I have suicidal tendencies, so I have to rethink what I'm doing. I keep a very strict separation between my school and private data footprint," said Kerrane, who is already taking an AP Computer Science class and aspires to work in coding or computer systems someday.

And, he said, it feels unfair that students who can afford to have personal devices of their own can more easily circumnavigate monitoring than students who have to rely on district-issued devices.

As both students and parents have discovered, the easiest workaround is to use a nonschool-issued device and log into a second account not tied to the school network. That typically isn't possible on a school-issued Chromebook.

The difference raises concerns about whether some groups of students are being observed more than others. The mistrust comes because by nearly all measures, disadvantaged students and, particularly, Black students are already monitored more than other students in other aspects of schooling, such as policing, disciplinary practices, and dress codes.

(Some districts like Oak Park that have "lease to own" programs for their school devices actually make more privacy an incentive. They offer parents who purchase the devices the opportunity to turn off filtering during nonschool hours.)

The loudest dust-ups about the classroom-management services, though, seem to have come from wealthier, more privileged communities. The Montclair, N.J., district, in early March temporarily halted use of GoGuardian Teacher in response to a parent outcry.

Are we conditioning students to surveillance?

For Vance, the privacy expert, it all comes down to context. In general, she worries less about remote classroom-management tools than the companies' other services, since there's at least a good case to be made that the management tools be useful in helping schools to fulfill their core job of teaching.

Still, communicating that to families can be done well or poorly, she said.

"Having someone come to you and say, 'I know what you were doing on the internet,' does not create a trusted relationship. So there's really a necessity to make sure that the monitoring that is occurring is really necessary and really fulfilling its purpose," she said. "Classroom-management software, when it's narrow and during class when students know about it, is going to be narrowly tailored. A lot of the other monitoring isn't."

Parents should also be informed what districts do with whatever metadata they collect via any of their online tools, where it's stored, and how often it's purged, she said.

And there are substantive differences in the services themselves. At least one other provider of remote classroom-management tools, Lightspeed, permits teachers to record students' screens, not just observe in real time. (Neither GoGuardian or Securly permits recording.)

Richardson, the Virginia teacher, concurs that it's partly her job to make sure students understand precisely what the program does. She thinks that's one reason her students are at ease with it.

"I made sure I told them about it at the beginning of the year, so it's very transparent that I'm using it," she said. "And I tell them I only use it while I'm in their class, so I don't do it from 8 in the morning to 5 in the afternoon."

At a broader level, it's still potentially worrisome that schools are layering so many student-surveillance tools on top of a social media ecosystem that already prioritizes oversharing, some privacy experts warned. Especially, they said, in the context of a tech-saturated world where everything from Alexa to home appliances is already potentially watching or listening.

"I just think we are all creating these environments where students think in this weird panopticon way that they're always being watched, and they can't expect any privacy under any circumstances," said Barbara Fedders, an assistant professor at the University of North Carolina School of Law, who wrote a 2019 law review article about the legal implications of surveillance for school districts.

(The panopticon refers to a prison design that, in theory, improves behavior among inmates because they don't know precisely when guards are monitoring.)

It's unclear yet whether surveillance could change students' behavior long-term, as the panopticon theory suggests, said Vance. It might alter their creativity and expressiveness in ways we don't understand, she said.

Or—and some research already suggests this is the case—perhaps students may simply assume that surveillance is everywhere, put it out of mind, and go back to behaving as usual.

At least for now, some parents say what they've learned about the classroom-management systems makes them wary. And they're still wrestling with the larger implications.

Carman's son is now logging into his remote schooling on a different browser. That means he can't access all the teacher-interaction functions that would be available to him in GoGuardian Teacher sessions, but his screen won't be watched.

Carman is troubled by the conversation he had with his son when he explained how the monitoring service worked: His son was not all that surprised.

"I'm realizing that with this generation—two if you count the millennials—not only do they not have this expectation of privacy, they don't even know what privacy means," he said. ■

—Getty

OPINION

Published on March 19, 2019

Why K-12 Cybersecurity Is Only as Good as the Leadership at the Top

By Doug Levin

Born in the 20th century, most superintendents and school board members are not experts in issues of technology, much less cybersecurity. As schools are growing increasingly reliant on 21st century technology for teaching, learning, and school operations, this lack of expertise has consequences and introduces new risks to school district operations.

Consider that of the 18 peer groups investigated by the Multi-State Information Sharing & Analysis Center in a recent review, local K-12 schools were reported to have the least mature cybersecurity risk-management practices of any state or local government agency. Similarly, a survey published last year by the National School Boards Association found that school officials are less prepared for cyberattacks than their peers in private sector companies.

As they juggle other critical priorities, superintendents and school board members may wonder what the scope of their responsibility should be in weighing cybersecurity risks and protecting against threats. After all, isn't that the purpose of cybersecurity insurance and the role of district technology staff? Why would district leaders be expected to do more? In what ways could they do more?

The hard truth is that we won't see fewer data breaches, fewer successful phishing attacks, and fewer ransomware incidents in schools until superintendents and school board members jointly embrace their cybersecurity governance responsibilities. Just as district leaders maintain the responsibility to manage risks to students' physical safety and health in the context of natural and man-made incidents, they also need to take a lead role in ensuring that their school systems are appropriately managing the digital risks to school communities introduced by the embrace of technology. These include risks to the confidentiality of data collected by school districts and their vendors, risks to the integrity (i.e., the accuracy and completeness) of that data, and risks to the availability of IT systems and data integral to the day-to-day experiences of students, teachers, and administrators.

There are three primary ways that superintendents and school board members—working in partnership with district technology staff—need to exercise their cybersecurity governance responsibilities.

"The hard truth is that we won't see fewer data breaches, fewer successful phishing attacks, and fewer ransomware incidents in schools until superintendents and school board members jointly embrace their cybersecurity governance responsibilities."

The first is via their ability to set priorities for their school district. Every district needs to develop, formally adopt, and implement a plan to manage the cybersecurity threats and risks they are facing. Such a plan should identify the district's critical IT and data assets, and detail how risks to those assets will be mitigated through policies, practices, and/or technology tools. It should explain for which risks insurance will be purchased, and—given that there are no 100 percent guarantees with cybersecurity—which risks will be accepted.

"The hard truth is that we won't see fewer data breaches, fewer successful phishing attacks, and fewer ransomware incidents in schools until superintendents and school board members jointly embrace their cybersecurity governance responsibilities."

In addition, a district cybersecurity plan should include procedures and guidelines for how the district will respond to cybersecurity incidents experienced by the district (or its vendors) when they inevitably occur. This is a question of liability—districts have been sued for negligent cybersecurity practices in the wake of significant incidents—as well as legal compliance under evolving federal and state privacy, cybersecurity, and data-breach notification laws. Indeed, district leaders would do well to anticipate that when their district experiences a significant data breach or cybersecurity incident, school community members, government agencies and law enforcement, insurance providers, and the media all will come to them seeking public answers and accountability.

Superintendents and school board members also need to show leadership on cybersecurity through their authority over the budget process. As part of their fiduciary oversight of school districts, superintendents and board members should be able to crosswalk their cybersecurity risk-mitigation plans to budget expenditures and track that spending over time. That is not to suggest that there is a magic dollar figure or percentage of a school IT budget that should be spent on cybersecurity-related activities as evidence of good practice. But by working with district technology staff to make explicit budget assumptions and expenditures, district leaders can ensure and document that cybersecurity measures are being supported and are keeping pace with emerging threats and protections. In cases where spending does not match the need, budget transparency can help garner the data necessary to re-allocate or seek out additional funding.

"District leaders would do well to anticipate that when their district experiences a significant data breach or cybersecurity incident, school community members, government agencies and law enforcement, insurance providers, and the media all will come to them seeking public answers and accountability."

Finally, superintendents and school board members need to put in place a process to assess the quality of their cybersecurity plans and spending at least once a year through clear organizational metrics. Such metrics should include—at a minimum—a reporting of the number, variety, and severity of cybersecurity incidents affecting or targeting the district and its vendors and partners, as well as one or more measures of the cybersecurity awareness of district staff. The process of determining and periodically tracking progress against a small set of meaningful metrics will go a long way toward moving cybersecurity risk management from district technology staff's hands alone to weaving it throughout the culture of the district.

District leaders are not only accountable to the public for managing cybersecurity threats; they are themselves disproportionately targeted by hackers. That means it's critically important for superintendents and school board members to set a good example via participation in cybersecurity training and awareness events and strict adherence to district policies.

Schools' reliance on technology for teaching, learning, and school operations will continue to grow. Every district needs to adopt a plan to manage cybersecurity risks, make sure they're putting the money and resources into supporting that plan, and track the success of their strategy over time. District technology staff can't do all of that work on their own. Superintendents and school board members should commit to creating a culture across their districts that anticipates cyber risks, rather than waiting to respond to attacks from malicious actors after the fact. ■

Doug Levin is president of EdTech Strategies, LLC and founder of the K-12 Cybersecurity Resource Center, which was launched in 2018 to shed light on the emerging cybersecurity risks facing U.S. K-12 public schools. He has been engaged in education and technology policy issues for over two decades in a variety of prominent roles, including serving previously as executive director of the State Educational Technology Directors Association.

Additional Resource

Federal agencies have warned schools to be on high alert for cyberattacks, especially since the pandemic forced more school operations than ever before into the digital realm. This downloadable timeline illustrates the long-term effects of a cyberattack and provides a roadmap schools can follow for responding to an attack.

Published by Editorial Projects in Education, Inc.
6935 Arlington Road, Suite 100
Bethesda, MD, 20814
Phone: (301) 280-3100
www.edweek.org

EducationWeek®

SPOTLIGHT

Get the information and perspective you need on the education issues you care about most with Education Week Spotlights

The Achievement Gap • Algebra • Assessment • Autism • Bullying • Charter School Leadership • Classroom Management • Common Standards • **Data-Driven Decisionmaking** • Differentiated Instruction • Dropout Prevention • E-Learning • ELL Assessment and Teaching • ELLs in the Classroom • Flu and Schools • Getting The Most From Your IT Budget • Gifted Education • Homework • **Implementing Common Standards** • Inclusion and Assistive Technology • Math Instruction • Middle and High School Literacy • Motivation • No Child Left Behind • Pay for Performance • **Principals** • Parental Involvement • Race to the Top • Reading Instruction • Reinventing Professional Development • Response to Intervention • School Uniforms and Dress Codes • Special Education • STEM in Schools • **Teacher Evaluation** • Teacher Tips for the New Year • Technology in the Classroom • Tips for New Teachers

VIEW THE COMPLETE COLLECTION OF EDUCATION WEEK SPOTLIGHTS

www.edweek.org/go/spotlights