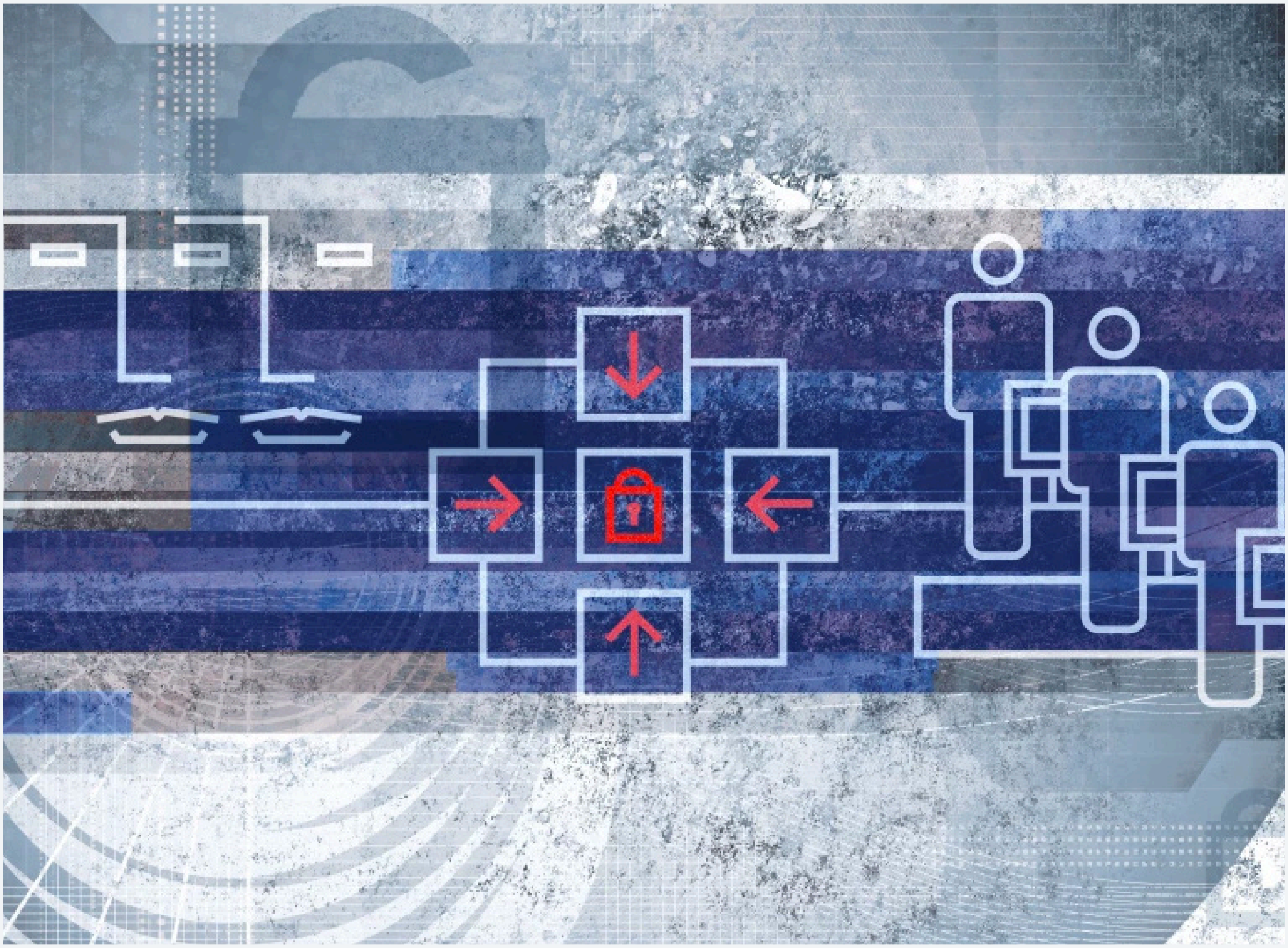
EducationWeek | SPOTLIGHT 2021



—Sean Gladwell/Moment/Getty

Lessons Learned: Digital Safety

EDITOR'S NOTE

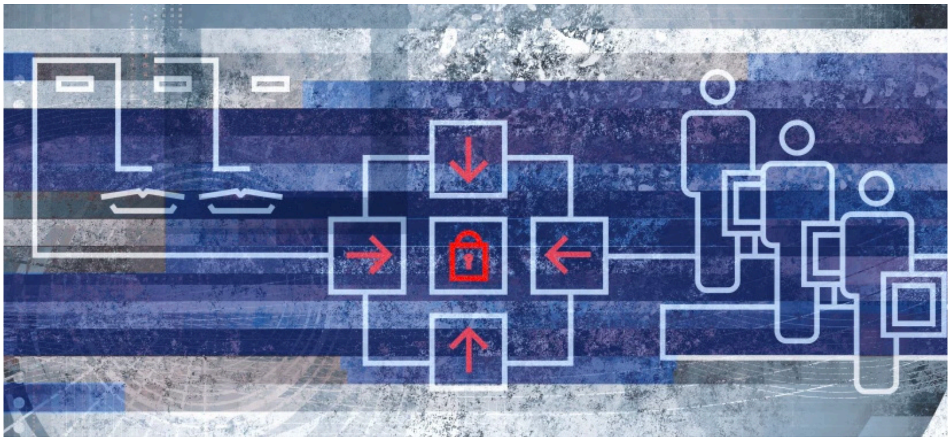
As summer begins, now is the time for educators to assess their own awareness of digital safety. In this Spotlight, review ways you should be approaching student and system data; discover what others have done to teach digital safety, and learn how some educators handled cyber attacks.

OPINION

Published on June 29, 2021

School District Data Systems Are Messed Up. A New Coalition Wants to Help

By Alyson Klein


—Sean Gladwell/Moment/Getty

Massive amounts of student information is being used to help school districts and states make all sorts of decisions these days. But the systems that collect and analyze that data are often, well, a bit of a hot mess.

Data systems are often splintered, meaning that educators are stuck spending hours putting together information from discordant systems or manually reentering information. What's more, now that student data is often stored in the cloud, privacy and security are paramount concerns. Cyberattacks against school districts are on the rise across the country.

Enter the International Society for Technology in Education (ISTE), the Council of Chief State School Officers, and the Council of the Great City Schools. The three organizations have tapped three state education agencies—in California, Massachusetts, and Nebraska—and 20 large school districts to join an effort to help make data systems more user-friendly, seamless, and secure.

The three-year partnership will help districts and states improve their systems' interoperability, meaning make it easier for disparate systems to communicate with one another. The goal will be to create a set of tools and processes that any state or district can turn to when looking to tackle incompatible systems and/or secure their data.

"We know that having access to the right data and right information is really powerful for educators to make those really informed decisions to support student learning," said Mindy Frisbee, the senior director of learning partnerships at ISTE, in an interview.

The partnership will give states and districts a chance to take a hard look at what data systems they already have and modernize their systems, in part to improve interoperability, Frisbee said. Districts and states will also get help in examining their procurement practices.

The aim is, in part, to support positive decision making around the adoption of educational technology tools, Frisbee said.

> "Data systems have always been foundational, but there's a better understanding now of just how much it matters for technology not only to function but to be properly integrated."
>
> **KENNETH THOMPSON**
> CHIEF INFORMATION OFFICER, SAN ANTONIO INDEPENDENT SCHOOL DISTRICT

District officials say the pandemic has put a spotlight on how important it is for data to be comprehensive and accessible.

"As a result of the pandemic, the role of data and technology infrastructure across the country has shifted," said Kenneth Thompson, the chief information officer for the San Antonio Independent School District, one of the 20 participating districts, in a statement. "Data systems have always been foundational, but there's a better understanding now of just how much it matters for technology not only to function but to be properly integrated."

Meanwhile, state officials say the project could help educators reclaim valuable time.

"Our continued work on Nebraska's interoperability plan will reduce the financial and human capacity burden on districts, which is more important now than ever," said Dean Folkers, chief information officer at the Nebraska Department of Education, said in a statement."Interoperability can be a highly technical and complicated subject, but at its core this work is about ensuring that teachers and parents have the information at their fingertips to support all students."

In addition to San Antonio, participating districts include: Albuquerque Public Schools, N.M.; Boston Public Schools, Mass.; Chicago Public Schools, Ill.; Clark County Public Schools, Nev.; Cleveland Public Schools, Ohio; Fresno Unified School District, Calif.; Dallas Independent School District, Texas; Hillsborough County Public Schools, Fla.; Kansas City Public Schools, Mo.; Minneapolis Public Schools, Minn.; Nashville Public Schools, Tenn.; Oklahoma City Public Schools, Okla.; Orange County Public Schools, Fla.; Philadelphia Public Schools, Pa.; Pinellas County Schools, Fla.; Portland Public Schools, Ore.; Rochester Public Schools, N.Y.;Saint Paul Public Schools, Minn.; Tulsa Public Schools, Okla. ■

netsweeper

Case Study

London Grid for Learning

A leader in student safety in the UK, used Netsweeper to scale their filtering service to protect over 2 million pupils

For schools, operational flexibility and ease of administration is the ultimate goal. IT managers and school administrators need a system that fits into their existing infrastructure and supports their student safety goals.

Company

The London Grid for Learning (LGfL) provides a filtered broadband connection, network services, online content, and support communities for schools across London.

Key Challenges

LGfL required an Internet content filtering solution that would provide the highest level of categorization accuracy and platform scalability. They also needed a solution that would provide the scalability and flexibility they needed as they expanded their services to 2000 schools and 2 million pupils. Key challenges include:

- Internet content filtering that didn’t interrupt the learning experience
- A network-based solution for filtering 2K+ schools, 2M+ pupils, and handle billions of URL requests a day
- Minimal network degradation and administrative overhead
- Easy to integrate with existing and planned management systems

Solution

Netsweeper deployed a high-performance filtering system that was adapted to the changing needs and increasing demands of LGfL’s massive customer base. The Netsweeper WebAdmin API has been used to develop a bespoke customer care portal for non-technical users to be able to manage their web filtering policies.

More recently, as the COVID-19 pandemic sent people home to work and study, Netsweeper was able to help LGfL rapidly roll out a comprehensive Chromebook and iPad filtering solution to over 100K pupils.

Results

Each policy server is load balanced, providing redundancy. Each school in the region is provided two policies - one for students, the other for teachers. Delegating admin rights to named staff at each school allows LGfL staff to create additional policies on an as needed basis. The accuracy of the solution has met the schools growing demands of Internet usage and met the expectations of BECTA (British Educational Communications and Technology Agency).

If you want to learn more about how nMonitor can help quickly identify when a student is at-risk, please visit www.netsweeper.com/nmonitor

— Getty

Published on March 17, 2020

How to Respond to a Ransomware Attack: Lessons Learned

By Alyson Klein

The Flagstaff Unified school district, back in September 2019, became one of more than 300 to suffer a ransomware attack that forced officials to close schools for two days and work around the clock to get everything back up and running.

Education Week chatted with Zachery Fountain, the Arizona district's director of communications, and Mary Knight, its director of technology, about what Flagstaff learned from the experience. This interview has been edited for length and clarity.

What exactly happened?

Fountain: We had a staff member who noticed something weird happening in terms of one of their processes, and they did the right thing and alerted IT. And IT promptly took action and was able to figure out that we had a case of ransomware that was a pretty nasty bug. We ended up going through the processes, evaluating what systems were impacted, what weren't impacted, and at the same time evaluating what systems did we need for school.

As part of our containment strategy, we needed to sever internet connections. It wasn't that we were locked out of all of our systems. It was that we made the decision to sever the internet and isolate the issue. We ended up canceling school for the next day [a Thursday] and then also on Friday to ensure that we were able to get everything up and clean.

[After] really a Herculean effort by our team here and also community organizations, we were able to get up and running for that following Monday. We were down for about four days, including two days on the weekend. But we were able to bounce back.

Knight: The most important thing is to have your backups in place. We were presented with email addresses for the ransomware but we did not contact them. We were fortunate that we had backups in place that allowed us to restore our systems.

What would you recommend to other districts to avoid paying a ransom?

Fountain: The big thing is having your team and your plans in place and prepare for not [just] an IT issue. It's a school system issue and how are people going to react? What does this look like in terms of instruction in the classroom if teachers can't get the data? What does it mean in terms of communication with stakeholders? There are going to be a lot of questions about general security. You just have to have all those things planned and know what your map is for your systems.

Knight: Have the resources that are required to help navigate through a situation like that. Most school districts don't have a cybersecurity expert on staff. You want to have [those relationships] in place, not be looking for someone when these events happen.

(The district is part of Arizona's "risk and retention" trust and had participated in its webinars and created an incident-response plan, she said.) "When we were working through this, we contacted the trust [a nonprofit corporation that provides the state's school districts and community colleges with property and liability coverage] immediately."

How did communications work?

Fountain: My biggest worry as communications director was that I didn't want to say something that would invite a secondary attack. We wanted to be very clear that we were dealing with a cyber issue that was ransomware. It wasn't a breach, so information wasn't taken off our server.

I did 37 interviews in 12 hours or something like that, with local media, national media, and international media. We really worked to make sure that our internal stakeholders had that information before we did things that were public. We want them to have a solid base of information before we send it out to everybody.

How else can districts get ready for an attack?

Knight: Prepare an incident-response plan and know who your incident-command team will be. Having those roles defined prior to an incident is critical. Backing up to cloud environments is also critical as well. It's important for schools to do an after-action review. You prepare, you have your response, and then you have your recovery and remediation.

As part of that recovery and remediation, you want to do an after-action review so you can process what occurred. This is a daily threat for everybody. It's something that has to remain on your radar constantly. You need to stay up to date on what's out there and learn from others. It's not something you can just create and put away and not worry about it.

You're constantly making those modifications so you can be as prepared as possible.

How long did it take for teachers to get back into instruction after being out for two days?

Knight: They were back at it Monday morning. Their laptops were all picked up, [and temporarily confiscated] and they got back to business. In our user agreement [for staff], it says we are not responsible for your data, that you need to be backing up your data. But for some people who hadn't backed up their personal data to the district network or a cloud-based option, they didn't have access to their data. For some, that didn't mean much, but for others, if it was 20 years of lesson plans, that was a little tough for those folks.

We all have to be very intentional about where we are saving our data to.

Any last pieces of advice?

Fountain: Celebrate the achievements along the way. The days are long. You've gotta be taking care of your staff. ■

— 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 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 cyberattacks

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 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 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. ■

— Diki Darmawan/iStock/Getty Images Plus

Published on March 6, 2018

Schools Teach ‘Cyber Hygiene’ to Combat Phishing, Identity Theft

By Sarah Schwartz

Students in Whitney Poucher’s cybersecurity education courses are no strangers to highly technical topics. At Greenbrier High School in Georgia’s Columbia County district, they learn how hackers monitor users’ systems to exploit weaknesses, and staff from the nearby U.S. Army fort drop in to give lectures.

But some of the most relevant lessons are also the simplest.

One incident at the school stands out in Poucher’s memory: A student opened another’s email account, impersonating that peer and sending a threatening email message to another classmate. The victim hadn’t logged out of an account on a public work station, which allowed the other student access.

Now, said Poucher, she makes sure to emphasize basic, practical security precautions—like logging out of public computers—in her courses.

Facing an increasing array of daily security threats, schools like Greenbrier are teaching what is being dubbed “cyber hygiene,” the basic cybersecurity habits that will keep students safe online at home and on their school networks. As reports of large-scale cyber attacks targeting business and government institutions have multiplied in recent years, cybersecurity education has come into national focus. Across the country, schools are implementing workforce-oriented courses to prepare students for careers in designing and protecting networks.

Profound Consequences

Cyber hygiene is foundational for students on these pathways, argue some educators and privacy advocates, though they also believe it has broader relevance. It’s not only IT specialists who deal with sensitive information online. Training in best practices can help middle and high school students protect their personal computers, understand the difference between ethical and unethical hacking, and prepare them to confront the digital threats they will face in the workplace.

At the same time, the challenge is to present lessons on cybersecurity habits in ways that engage, rather than overwhelm, students and resonate with their daily experiences, educators and advocates say. Teachers also say there’s a need to remind students of the ethical choices that come with making decisions about how they use technology.

Cyber Safety Habits Curricula

National Integrated Cyber Education Research Center: The project, funded by the federal Department of Homeland Security and based out of Louisiana’s nonprofit Cyber Innovation Center, offers free K-12 cybersecurity curricula to schools and districts. Courses at the high school level include Cyber Science and Cyber Society. They cover everyday safety risks, cyber law, and online ethics.

Common Sense K-12 Digital Citizenship: Common Sense Media includes lessons on privacy, security, and internet safety in their broader digital citizenship curriculum. Topics covered at all grade levels include identifying spam, creating strong passwords, and figuring out whether a website is protecting users’ personal information.

CyberPatriot Training Modules: CyberPatriot, a cyber education program created by the Air Force Association, aims to encourage students to pursue careers in cybersecurity or STEM fields. Training materials for the program’s national IT simulation competition for middle and high school students include tips on protecting personally identifiable information, instructions on building strong passwords, and case studies on ethical cyber behavior. Archived training modules are publicly available on the CyberPatriot website.

Elementary School Cyber Education Initiative: Also developed by CyberPatriot, these three free digital games are designed to teach students in grades K-6 about online safety and introduce them to the basics of cybersecurity. The games, available in English and Spanish, cover topics like phishing, malware, security software, and sharing personal information.

iSAFE Digital Citizenship: iSAFE, a nonprofit publisher, offers digital curricula for grades K-12 covering a range of privacy, security, and digital citizenship topics. Lessons in digital safety and security summarize broad subjects like personally identifiable information and acceptable use policies, but also touch on specific issues relevant to teenagers' lives—for example, risks to watch out for when shopping online.

As targeted cyberattacks, like phishing, become more sophisticated, schools have a vested interest in helping take security precautions, said Jonathan King, the chief strategy officer at i-SAFE, a provider of curricula on cybersecurity, privacy, and digital citizenship. Counting teachers, administrative staff, students, and parents, districts have an "inordinate" amount of users on their systems, said King.

"Anything they can do to help mitigate irregular use on their infrastructure helps them in the long run," he said.

As soon as students begin using devices in the classroom, teachers and administrators need to start having age-appropriate discussions about staying safe and protected, said Kevin Nolten, the director of academic outreach for the National Integrated Cyber Education Research Center. The center develops cybersecurity curricula for schools to integrate across disciplines.

"When I walk into a kindergarten class, and they have a set of iPads that they're utilizing, we need to begin having a conversation about security," said Nolten.

At that age, he said, teachers can talk with students about the purpose and use of passwords, and other, broader questions. Why do we secure certain information? Why might we want a private space online?

When they're working with older students, teachers can draw connections to current events. Poucher said she keeps her high school students up to date on news about ever-evolving cyber attacks, like phishing scams, that could target them at home or at school. "The best defense," she said, "is understanding the offense."

Drawing direct connections to situations that users could actually experience makes cybersecurity warnings stick, said Michelle Mazurek, an assistant professor in computer science at the Institute for Advanced Computer Studies at the University of Maryland, College Park. That's why demonstrating the consequences of a specific action, like leaving an account open on a public computer, is a good strategy, said Mazurek, whose research is focused on building systems to support users' security and privacy behaviors and preferences.

Cyber Safety Habits Curricula

National Integrated Cyber Education Research Center: The project, funded by the federal Department of Homeland Security and based out of Louisiana's nonprofit Cyber Innovation Center, offers free K-12 cybersecurity curricula to schools and districts. Courses at the high school level include Cyber Science and Cyber Society. They cover everyday safety risks, cyber law, and online ethics.

Common Sense K-12 Digital Citizenship: Common Sense Media includes lessons on privacy, security, and internet safety in their broader digital citizenship curriculum. Topics covered at all grade levels include identifying spam, creating strong passwords, and figuring out whether a website is protecting users' personal information.

CyberPatriot Training Modules: CyberPatriot, a cyber education program created by the Air Force Association, aims to encourage students to pursue careers in cybersecurity or STEM fields. Training materials for the program's national IT simulation competition for middle and high school students include tips on protecting personally identifiable information, instructions on building strong passwords, and case studies on ethical cyber behavior. Archived training modules are publicly available on the CyberPatriot website.

Elementary School Cyber Education Initiative: Also developed by CyberPatriot, these three free digital games are designed to teach students in grades K-6 about online safety and introduce them to the basics of cybersecurity. The games, available in English and Spanish, cover topics like phishing, malware, security software, and sharing personal information.

iSAFE Digital Citizenship: iSAFE, a nonprofit publisher, offers digital curricula for grades K-12 covering a range of privacy, security, and digital citizenship topics. Lessons in digital safety and security summarize broad subjects like personally identifiable information and acceptable use policies, but also touch on specific issues relevant to teenagers' lives—for example, risks to watch out for when shopping online.

"If you hear a story about something that went wrong, and you say, 'I would never do that,' that's less effective," she said.

But one of the risks in cyber-education programs—for students or adults—is that the audiences are overloaded with warnings and other information, Mazurek said. People have "limited bandwidth" to make changes in their daily routines, even if they know what security precautions they should be taking, she said. Focusing on a few crucial, actionable steps—generating strong passwords, updating software, being cautious of scams—makes it more likely that people will actually follow advice.

In the Bossier Parish school system in Louisiana, many students get those types of lessons through the CyberPatriot program, a national competition for middle and high school students run by the Air Force Association. Students practice in local teams to run an IT simulation, in which they manage the network of a small company. The district also offers cyber literacy and cyber science electives, taught with National Integrated Cyber Education Research Center curriculum materials, for high schoolers, and fields CyberPatriot teams at the middle and high school level.

Parsing Cyber Ethics

Lessons that prepare students for the competition touch on topics like how to craft a strong password, safe browsing tips, and websites that pose security risks (online shopping and social media are at the top of the list).

A step-by-step guide on spotting phishing attempts shows a sample email and labels the telltale signs: Messages are sent from a spoofed sender address, and generally ask the recipient to click through a link to input personally identifiable information.

For most of the students she's worked with, these warnings are new information, said Charlene Cooper, an instructional coach at Cope Middle School in the Bossier Parish system and a CyberPatriot coach.

Most students don't immediately make the connection that the kinds of cyber attacks unleashed on banks or government agencies could happen closer to home, said Marco Reyes, a cyber literacy teacher at Bossier High School.

Learning about attacks and security in school settings make it clear that these are concrete concerns, with profound consequences, he said.

Those consequences are especially apparent when the school is the site of an attack.

A few years ago, Nathan Mielke was getting ready for a cybersecurity-themed homeroom lesson at Hartford Union High School in Wisconsin. A few minutes after the period was supposed to start, a distributed denial-of-service, or DDoS, attack cut off access to the internet.

Mielke, the director of technology services in the high school district, said that to this day, leadership isn't sure whether a student or an outside actor was responsible.

"But I will tell you that after we talked to students face to face about it, it stopped," he wrote in an email.

He used the network failure as a teachable moment, explaining what happened and how the attack blocks internet connectivity, in follow-up announcements and in the school newsletter.

Grounding cybersecurity lessons in conversations about right and wrong can steer students away from mischief-minded experiments, said Nolten, of the national research center.

"It's not only important to teach a student how to push the gas pedal," he said. "We've also got to teach them how to push the brake."

In Columbia County, Ga., Poucher teaches her students how to use a virtually protected network, or VPN, which allows users to securely access a private network and still share data through public networks. Protected networks can insulate users from hackers and surveillance online, Poucher explains to students, so they can be a safer alternative to public networks at coffee shops and hotels.

But she stresses to her classes that using the same technology at school can violate district policy, because it can be used to bypass the school's internet filtering software. In that case, she said, students would be trying to avoid protections put in place by administrators meant to keep them safe.

In Poucher's classes, students learn how to parse the sometimes messy distinctions between moral and immoral, and safe and risky, behaviors.

"Teaching them the responsibility that they have over themselves," she said, "is huge." ■

Published on March 17, 2020

4 Big Cybersecurity Priorities for Schools: Training, Purchasing, Monitoring, and Budgeting

By Mark Lieberman

Cyberattacks are on the rise in computer networks across the country, leaving many schools scrambling to contain threats and educate communities on device etiquette. To get a better sense of what's working to address this challenge, Education Week partnered with the Consortium for School Networking, or CoSN, to survey 513 K-12 technology leaders on how they are dealing with the latest cybersecurity challenges. Education Week followed up with interviews of chief technology officers to better understand what approaches are working to curb and clean up cyberattacks. Here are four key areas ed-tech leaders should address:

Training

The survey of K-12 technology leaders featured a list of techniques for dealing with cybersecurity challenges, asking them to mark "yes" for the ones that apply and "no" for the ones that don't. Techniques involving training ranked highest: **77 percent of respondents said they're training IT staff, 69 percent said they're encouraging staff members to upgrade passwords, and 63 percent said they're working on training end users, such as teachers and students.**

— Getty

In 2019, Keith Bockwoldt was promoted to chief information officer for Hinsdale Township High School District 86 in Illinois. Only a few months after he started in the role, a teacher clicked on an email that purported to be from a former student. It ended up creating a malware infection that required Bockwoldt to tap into cybersecurity insurance for the first time in his 21 years working in the district.

That experience underscored for him the importance of arming teachers with knowledge of real-world situations in which they can play a major role. Bockwoldt started offering lessons to teachers during their prep periods, showing them videos that opened a window into a day in the life of a hacker.

"They were like, 'Wow, that really happens,' " Bockwoldt said. "It really gave them an awareness."

Bockwoldt naturally has had more success getting through to teachers when he speaks "in layman's terms" rather than overloading them with tech jargon. He also recommends getting the board of education involved in the discussions.

Melissa Tebbenkamp, the director of in-

Tackling the Student Mental Health Crisis

A students' life can be a never-ending array of ups and downs and heartbreak. While these life phases are inevitable and accepted as a normal part of growing up, there are instances when shifts in mood and behavior may be indicators of a larger, more daunting issue: mental illness. The number of student's today experiencing mental health issue continues to rise. Close to 20% – one in five – students are actively dealing with a mental health issue.

In February, Reuters surveyed school districts nationwide to assess the mental health impacts of school shutdowns because of COVID-19.

Of the districts that responded, 74% reported multiple indicators of increased mental health stresses among students. More than half reported rises in mental health referrals and counseling.

Almost 90% of responding districts cited higher rates of absenteeism or disengagement, signs that often point to potential issues with student emotional health. More than half of the districts reported that in person education was a driver of these warning signs of trouble.

More than ever, it's crucial that we eliminate the stigma and fear surrounding mental health, while starting helpful dialogues that will benefit students now and in the years to come.

> ***"Close to 20% - one in five - young people are actively dealing with a mental health issue."***

Identifying At-Risk Students

Mental health disorders in students is a complex issue that requires a coordinated effort and multilevel approach from parents, schools, and health care organizations to digital media outlets and community outreach. Early detection and intervention are crucial factors in the goal towards reaching at-risk students before conditions manifest into more serious issues.

Netsweeper, a leading provider of education web filtering solutions for over 20 years, is committed to on-going efforts to provide educators with the technology tools to not only limit students' exposure to harmful online content but also proactively gain insight to online behavior cues that signal at-risk conditions so that steps can be taken proactively to ensure early intervention. nMonitor, part of the Netsweeper Education Platform, scans content on students connected devices looking for words and phrases that could indicate issues relating to depression, suicide, cyberbullying, and more and alerts administrators with the information they need to take appropriate action.

If you want to learn more about how nMonitor can help quickly identify when a student is at-risk, please visit www.netsweeper.com/nmonitor.

structional technology for the Raytown Quality schools in Missouri, said her team tries to engage teachers with humor, tossing memes into short weekly emails to keep the issues top of mind throughout the year.

Training has made a difference, Bockwoldt said. He's started getting more suspicious emails forwarded to him from teachers who haven't opened them.

Purchasing

Tackling cybersecurity often means acknowledging areas where the school needs outside help. **Sixty-three percent of respondents to the CoSN/Education Week survey said they're purchasing specific cybersecurity products and services.**

Diane Doersch, who retired who retired in 2019 as chief technology and information officer for the Green Bay public schools in Wisconsin, likes the tool ClassLink, which provides single sign-on infrastructure for online applications, keeping the data secure. In general, she found that the most valuable way to get the most out of products was to meet regularly with the companies that provide them.

"I had quarterly meetings with the company that provided our firewall," Doersch said. "They had the very specifics on how many times your district was pinged by a foreign nation."

Tebbenkamp is less bullish on the potential for outside companies to help schools. "There's a lot of products and services out on the market that aren't a good fit for us," she said. "Every district should take the time to evaluate whether it's a good fit."

She's found that many existing products have cheaper open-source alternatives. Sometimes, an investment is worthwhile, such as an intrusion-detection system that scans her district's online traffic, identifies threats, and paints a picture of the district's normal traffic patterns. Tebbenkamp said the investment was small but the district got a lot out of it.

Monitoring

More than half of survey respondents said they're engaged in real-time monitoring to detect security threats. School networks present an overwhelming amount of information, Tebbenkamp said. It's important to prioritize—she deputizes two people each morning to look at dashboards, scan daily reports, and flag items that appear out of the ordinary. Part of her team combs through news threads and weekly briefings; if one person doesn't catch something, another might.

"I think the biggest piece is what data do you really need to be looking at. You need to establish: What logs should you be collecting and reviewing? What network activities do you need to be monitoring?" Tebbenkamp said. She's also resigned herself to accepting that "something slips through the cracks" no matter how much monitoring takes place.

Budgeting

Resources are always at a premium in K-12 schools, which means finding adequate funds for cybersecurity initiatives can be challenging. **Only 12 percent of survey respondents said their district has a budget line item for cybersecurity, and just 20 percent have created a cybersecurity team.**

Tebbenkamp said in a perfect world, she would add a chief privacy officer, rather than having her network system administrator lead her security team, and hire a data-security specialist. More cybersecurity experts couldn't hurt, she said. But she's found success with designating a "core group of individuals" on her broader team who have cybersecurity among their duties.

"They're not going to have all that knowledge, so you need all of your key knowledge stakeholders to be part of a team so you're not making decisions in isolation," she said.

Added Hinsdale High's Bockwoldt, "I've seen that happen at so many places: You didn't have the processes in place to take care of it. All of a sudden, something bad happens, you're throwing all kinds of money at it," he said. "Having that conversation at a cabinet level is extremely important." ■

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 is still unfolding, they should be looking out for signs of students engaging in digital self-harm, researchers say.

A 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.

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.

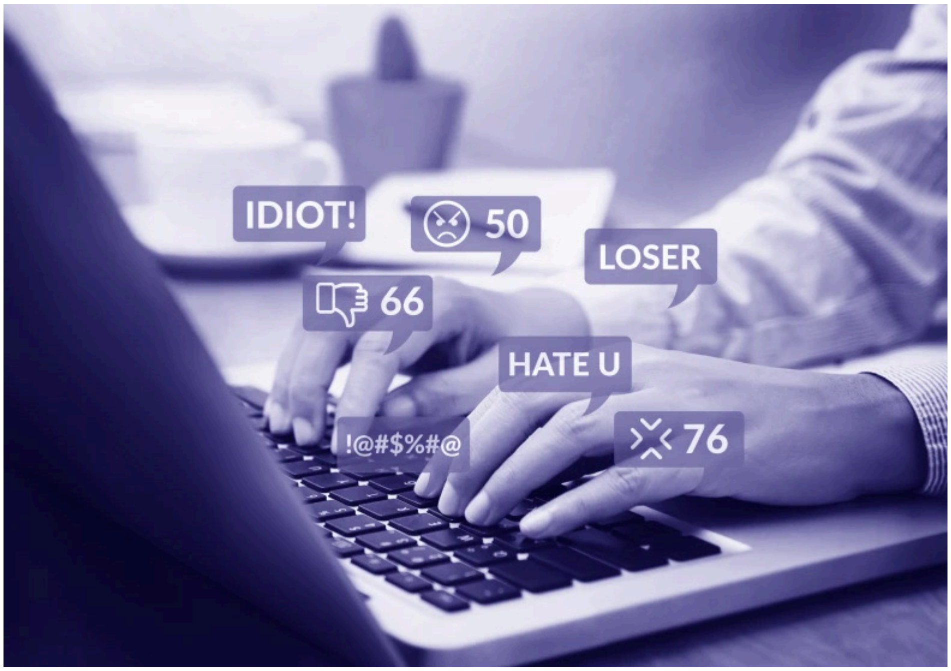
We had been studying cyberbullying among adolescents for probably a decade at that point, and we hadn't considered that students would send hurtful messages for themselves. We looked around [to see] if anybody had done any research on it. There were a couple of blog posts speculating, but that was about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

In 2016, we surveyed 5,500 12 to 17-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 depressed, 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.



— iStock/Getty

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.

> “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. ■

Additional Resource
[Cyberattacks Are on the Rise. Here's How Schools Should Respond (Downloadable Guide)]

—Vanessa Solis/Education Week, Akindo/Getty

OPINION

Published on January 30, 2020

The Cyber-Security Problem Schools And Ed. Tech Need to Face

Thousands of students had private data compromised last year. We must do better

By Joel Schwarz

We have seen story after story that detail breaches of educational technology vendors' system security. These troubling incidents in which sensitive student data is compromised will only become more frequent until both technology companies and public school districts make student privacy and security a greater priority.

Bethesda Magazine reported on a breach of student data held on behalf of Montgomery County public schools in Maryland by Naviance, an ed-tech provider used by middle, high school, and college students that collects students' dates of birth, ethnicity, test scores, and other sensitive data. Far larger than initially believed, the data breach affected close to 6,000 students.

How did the hacker breach Naviance? In layman's terms, the student hacker committed a "brute force" attack, akin to attempting to break into a house by jiggling every door and window looking for vulnerabilities. Specifically, the hacker used a script to iteratively try to log into accounts, looking for instances in which the user ID and passwords were the same, likely running the script thousands of times to get access to the almost 6,000 accounts. Unfortunately, Naviance didn't announce the full scope of these intrusions until months later.

Even without catching these access attempts (something a good cyber-security framework would have remedied), the hacks still would have failed if Naviance had implemented better password security. The hacker exploited a vulnerability—use of the same string for user ID and password—that most websites prohibit. Because Montgomery County student IDs are accessible to all district staff and students cannot change them, only strong password policies could have protected the accounts.

Even worse, this was actually the third Naviance breach in 2019; the first was a data breach in Virginia, where a parent was mistakenly allowed access to sensitive details of 21 former students. And then, in Pennsylvania, a group of high school students gained access to more than 12,000 students' addresses, student identification numbers, grade point averages, and SAT scores just to gain an edge in a competitive water-gun fight.

But Naviance wasn't the only ed-tech vendor to deal with student data breaches in 2019. The ed-tech vendor Pearson confirmed that it had suffered a security breach of the system it uses to monitor academic progress, affecting approximately 13,000 school and university accounts. Each account held by a school district provided access to potentially thousands of students' names, birth dates, and email addresses. And like Naviance, Pearson didn't detect the breaches until months after they occurred. Moreover, the Pearson breach included student data dating back to 2008, meaning that had it been promptly deleted after those students were no longer enrolled, the breach would have had a far smaller impact.

Also seen in 2019 was a breach of student data through a K12 Inc. learning software application used by more than 500 school districts, which left the personal records of 19,000 students exposed on an unsecured cloud server.

Most significantly, there are a number of basic cyber-security steps that could've been taken to prevent these breaches, including:

- Continuous, real-time monitoring of access attempts, which would've detected the unsuccessful log-in attempt missed by both Naviance and Pearson;
- Strong password policies, prohibiting the use of the same value for both user ID and password;
- Regular compliance monitoring to include spot checks and audits to identify repeated access attempts, repeated accesses of different accounts from the same IP address, unauthorized accesses, and violations of password policies. This could've likely prevented the breaches at all three ed-tech vendors;
- Timely deletion of student data when it is no longer needed to fulfill the business purpose; and
- Maintenance of data in a secure, password-protected environment which is encrypted at rest, so even if stolen, it's indecipherable.

These items are already covered in many cyber-security frameworks currently available, such as the National Institute of Standards and Technology's Cybersecurity Framework which has been widely adopted by the private sector.

> “If we do nothing, we should expect nation states to begin targeting our students through ed-tech vendors' systems. After all, the students of today are our government leaders and captains of industry tomorrow.

Finally, it's worth noting that of the three vendors discussed, only Naviance took the Future of Privacy Forum's Student Privacy Pledge, agreeing to “maintain a comprehensive security program that is reasonably designed to protect the security, privacy, confidentiality, and integrity of student personal information against risks—such as unauthorized access or use, or unintended or inappropriate disclosure.” In other words, two of the three ed-tech vendors were not even willing to commit to security precautions that could've prevented the breaches discussed above.

Then again, good intentions alone don't protect our children's personally identifying information. Even though Naviance took the pledge, they clearly failed to abide by it, highlighting the ultimate shortcoming of the pledge and an urgent need for greater accountability.

With or without the Student Privacy Pledge, the only way to truly ensure the privacy and security of our children's information is for ed-tech vendors to put their money where their mouths are and implement stronger security controls. Likewise, vendors need to implement a robust compliance monitoring program, including regular audits and spot checks. And they need to make the results of those reviews public, so that we can draw our own conclusions. Only through implementation of a compliance program—and transparency of the results—can ed-tech vendors begin to earn back our trust.

School districts must also do their part to help students protect themselves, such as through the use of de-identified accounts (an option that Montgomery County public schools already offers on an opt-in basis, but needs to be more widely publicized), which would minimize the harm of data breaches. School districts should also incorporate explicit compensation for students and penalties for ed-tech providers into vendor contracts, so that when a breach does occur, the vendor is held accountable.

If we do nothing, we should expect nation states to begin targeting our students through ed-tech vendors' systems. After all, the students of today are our government leaders and captains of industry tomorrow. They are an attractive target for a country like China, for example, which has the patience and strategic focus to plan ahead.

As a parent and a cyber-security professional, I'd prefer my children's data not go down this path. It's up to ed-tech vendors to step up and be proactive about delivering on their obligations. ■

Joel Schwarz is a senior principal at Global Cyber Risk, where he works as a consultant and attorney, and an adjunct professor at Albany Law School. He previously served as the Civil Liberties and Privacy Officer for the National Counterterrorism Center and was a cybercrime prosecutor for the Justice Department and the New York State Attorney General's Office, and Counsel on E-Commerce and Privacy for MetLife.

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

Impacts of COVID-19 on Education
Educational Technology
Remote Instruction and Interventions for Learning Loss