—Getty

Cybersecurity

EDITORS NOTE

Cybersecurity and privacy disruptions occurred in education well before instruction moved online. In this Spotlight, learn how educators are combatting cyberattacks, strengthening district-wide cybersecurity efforts, and training school employees to prevent cyberattacks.

OPINION

Published on September 14, 2020, in Education Week

Cyberattacks Disrupt Learning Even More During COVID-19

By Alyson Klein

Just two weeks into the school year, the Rialto schools in California had to shut down virtual instruction for a week due to a malware attack.

Designed to disrupt or gain access to a school's network, the malware attack also forced the 25,500-student district to collect–and fix–thousands of school-issued digital devices. Staffers wore masks and gloves as they worked, to protect themselves from potential COVID-19 infection.

Cyberattacks on school districts are nothing new. In fact, there have been nearly a thousand such incidents since January of 2016, according to the K-12 Cybersecurity Research Center.

But, as schools nationwide are engaged in full-time remote instruction or a hybrid of in-person and virtual learning, such attacks are arguably even more disruptive, both to students' educational as well as social and emotional needs.

"I thought to myself, why would somebody do this to students? They are already going through so much," said Syeda Jafri, a spokeswoman for the Rialto district. She noted that many children in the district had lost a relative to the virus or had someone close to them get very sick. "COVID is disheartening enough for children. It's just one more layer of chaos that could have been eliminated."

What's more, with so many students taking classes only from home, a cyberattack can have an outsized impact on schooling.

"If a school experiences a cyber incident and even a significant one in normal times, you still have a teacher in the classroom with students," said Doug Levin, the founder and president of the K-12 Cybersecurity Resource Center. In that scenario, teachers "may not be able to follow their lesson plan, but can still do valuable things with that time. But if a cyber incident occurs in times of remote learning, the loss of that online access stops teaching and learning in its tracks."

Plus, cyberattacks compound what is already a tense and difficult time for schools. "Everybody is on edge and has very little tolerance for these sorts of disruptions," Levin said.

—Getty

> "I thought to myself, why would somebody do this to students? They are already going through so much. COVID is disheartening enough for children. It's just one more layer of chaos that could have been eliminated."
>
> **SYEDA JAFRI**
> A SPOKESWOMAN FOR THE RIALTO DISTRICT, CALIFORNIA

Not only are cyberattacks more troublesome at a time when virtual learning is at its peak, they appear to be on the rise since the beginning of this school year, said Levin, who has been tracking cyberattacks on schools since early 2016.

So far, there have been 220 attacks for the 2020 calendar year, compared with 348 for the full 2019 calendar year. But the start of the school year is bringing a wave of new disruptions, Levin said. "The cyber hackers are back at work," he said. "Since Aug. 1, I'm seeing a spike for sure."

This school year, Levin says, there have been, on average, two hacks a day. That's unusually high, even for the start of a school year, when hacks tend to spike, he added.

Preparing for Cyberattacks

So how can school districts prepare for the possibility of an attack?

Levin suggested including not just IT staff, but the legal counsel and public relations department in creating a plan for how to handle a cyberattack. Districts should also know who their law enforcement contacts are, and consider having a cybersecurity firm on retainer that can help with recovery and forensics.

And he suggests that districts advocate for resources to help build up their IT capacity, team up with nonprofits for cyber security monitoring, and partner with other school systems.

Communicating clearly with parents, teachers, and the community is also key, said Patty Mazur, a spokeswoman for the 25,000 student Toledo school district in Ohio, which experienced an attack on Sept. 8, the first day of school. At the time, teachers were working from their classrooms in school buildings, while students were home, online.

The district recognized almost immediately that something was up.

"Around noon, we started hearing from schools that were losing their internet connection," said Mazur. Some teachers were able to continue instruction using hotspots, but many had to stop teaching.

The district quickly launched a forensic search of its computer system. The pause in learning was relatively short-lived, with classes fully back online about a day and half later. The district also contacted the FBI, which is looking into the attack, Mazur said.

"It was just one more challenge that COVID-19 has put in our paths for getting ready for the 2020-21 school year," Mazur said. Her advice to other districts: Put out crisp, accurate infor-

Learn. Anywhere.

http://aka.ms/securityedu

As schools around the world work to reimagine education, it's become more important than ever to make technology accessible, safe, and engaging for all students and educators. Affordable and secure Windows 10 devices are built for education to create a consistent learning experience no matter the environment—remote or hybrid.

With affordable and secure devices, powerful tools for education, and free professional development opportunities, Microsoft is here to support your educators in creating safe, inclusive online environments that help every student to learn anywhere.

Microsoft

mation on the problem for the public. "Stay on top of it, be upfront," and be sure that you have all the facts straight, so that you don't have to backtrack, she said.

'It Is Disheartening'

In Connecticut, the 18,000-student Hartford Public Schools had planned to open on Sept. 8, for both in-person and online instruction. But the district suffered a malware attack that disrupted the system the district uses to communicate transportation routes with its bus company, Leslie Torres-Rodriguez, the district superintendent, told NBC Connecticut. The district's learning management system wasn't affected, she said. Hartford was able to resume classes the following day.

Sometimes, students are behind the attacks. That was the case in Miami-Dade, the nation's fourth largest district, which experienced a spate of technical glitches in its first week of instruction, beginning Aug. 31. A 16-year-old student used an online application to carry out the attacks and has been charged in connection with them, according to a statement from the 345,000-student district.

"It is disheartening that one of our own students has admitted to intentionally causing this kind of disruption," said Superintendent of Schools Alberto M. Carvalho in a statement.

And in Virginia, the state's largest system, Fairfax County Schools, was hacked this month. The attackers are asking for a ransom payment. They have threatened to disclose personal information, including student disciplinary records and grades, according to WRC-TV in Washington. The 187,000-student school system is working with law enforcement to resolve the problem.

Smaller districts haven't been immune from cyberattacks, either. The 7,000-student Haywood school district in North Carolina's Appalachian Mountains, had to pause its all-virtual instruction for a week, due to an attack that is now under federal investigation.

The superintendent, Bill Nolte, suggests that districts make sure their networks are in good shape before an attack happens, since that will make an attack easier to fix. And he urges districts to "call on every available resource"–local, state, and federal–to fix the problem.

"Things happen and the question is: how do you respond?" he asked. ■

Published on October 15, 2020, in Education Week's Digital Education Blog

Large, Well-Off Suburban Districts Most Likely to Get Hacked

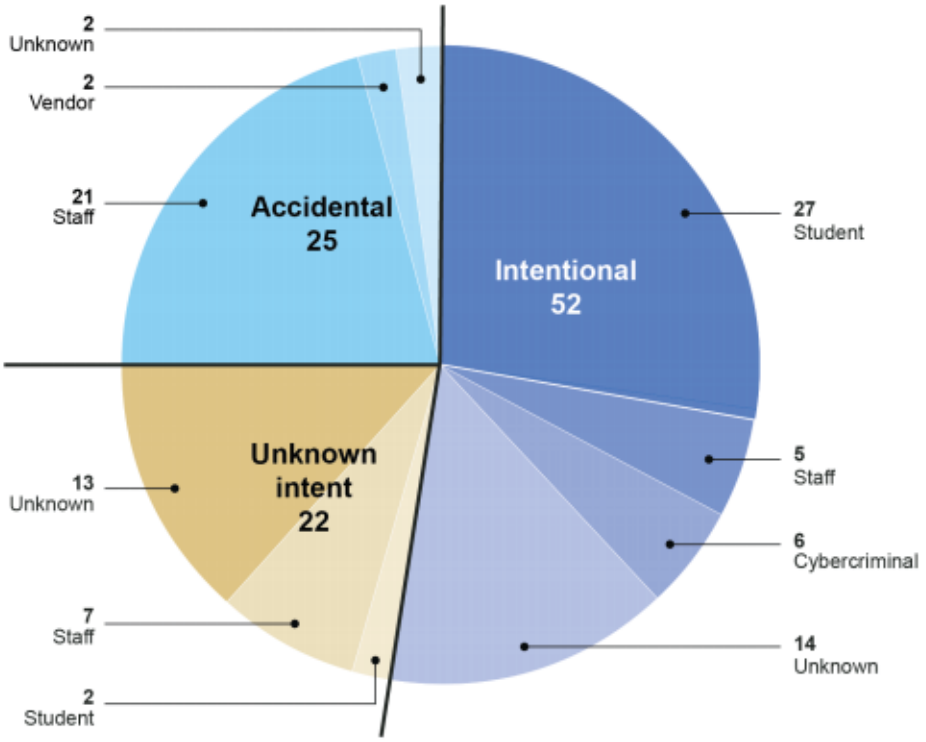
By Alyson Klein

Big. Wealthy. Suburban. Those are the school districts most likely to report a data breach, according to a report released Thursday by the Government Accountability Office, Congress' investigative arm. Cybersecurity is an especially sensitive issue right now, as schools around the country are operating virtually to avoid spreading COVID-19.

The agency found that districts where 25 percent or fewer students are eligible for free or reduced-price lunch comprised 26 percent of reported breaches, although they make up only 15 percent of all districts across the country.

And it found that suburban districts were more likely to be the target of attacks than urban or rural districts. Suburban districts made up 61 percent of districts with breaches, although they are only 39 percent of school districts overall. On the other hand, rural districts

Figure 4: Reported Number of K-12 Cybersecurity Student Data Breaches by Actor and Intent, July 1, 2016-May 5, 2020



Source: GAO analysis of K-12 Cybersecurity Resource Center data. | GAO-20-644

Notes: The actor responsible for a breach or the intent may be unknown from the details provided in public reports.

For this analysis, a cybercriminal is defined as an actor external to the school district who breaches a data system for malicious reasons.

comprised 21 percent of districts with reported breaches even though they make up 42 percent of school districts overall. Urban districts comprise 19 percent of all districts, but 17 percent of districts with reported data breaches.

What's more, larger districts also tend to be targets of reported attacks more often than smaller districts. School districts with fewer than 1,000 students comprise 60 percent of all districts, but just 18 percent of those with reported hacks. Meanwhile, districts with more than 10,000 students make up just 5 percent of districts overall, but comprised 30 percent of reported hacks,

Why might that be? Experts who spoke to the GAO said that, for one thing, it might be easier to target larger districts since they are likely to have more staff members and, therefore, more people to respond to a potential phishing email. And bigger, wealthier districts are more likely to use more technology than smaller, poorer districts, which also provides more opportunities for a breach. Wealthy, large, suburban districts are also more likely to have people constantly monitoring their networks (such as a chief technology officer) and may notice an attack which less well-resourced district may not.

More than half of data breaches are intentional, the report found, while about a quarter are accidental. When the breach was intentional, students were most often responsible. And grade changes were the most common motivation. When the breach was an accident, staff were most often responsible. For instance, staffers might email data to the wrong recipients or post it on a public website, which is considered a breach.

The GAO's analysis relied on data from the K-12 Cybersecurity Research Center. ■

Published on July 14, 2020, in Education Week's Digital Education Blog

Congress Heightens Emphasis on K-12 Cybersecurity During COVID-19

By Hannah Farrow

Federal lawmakers put a new focus on improving cybersecurity, including protections for schools, through a pair of measures aimed to create more leadership at the national level and encourage safeguards in classrooms.

One bill introduced in June 2020, the National Cyber Director Act, seeks to appoint a federal cybersecurity director who would oversee cyber safety and regulations nationwide. The nominee would lead a strategy to address security risks in the U.S. cyberspace.

Another piece of legislation, the Providing Resources for Ongoing Training and Education in Cyber Technologies, or PROTECT Act, would help support the Department of Homeland Security's Cybersecurity Education and Training Assistance Program (CETAP) to promote career awareness, provide resources, and help to develop the cybersecurity skills of students in elementary and secondary schools across the country.

The bipartisan bill was introduced in early July by Sen. Jacky Rosen (D-NV) and Sen. Bill Cassidy (R-LA).

"The current cybersecurity workforce shortage poses a threat to our national security. To meet this challenge and prepare our nation for the economy of the future, we must invest in a robust cybersecurity workforce," Sen. Rosen said in a news release. "This bipartisan legislation would codify and strengthen the CETAP program, providing education and career opportunities in cyber and helping to bolster the number of applicants in this critical field."

> "School district IT systems are interconnected with other local state and federal systems, including voting systems, law enforcement, systems that have to do with employment and commerce."
>
> **DOUG LEVIN**
> PRESIDENT, EDTECH STRATEGIES

The PROTECT Act would "authorize and provide stability" to the CETAP program, seeking to implement the Cyber-Integrated Curricular Model (CICM) in schools, which provides hands-on, cybersecurity-integrated tools and introduces students to the cybersecurity profession. It also helps elementary, middle, and high school teachers develop their teaching abilities around cybersecurity issues.

As for the National Cyber Director Act, the Cyberspace Solarium Commission recommended the measure based on a report published in May, Cybersecurity Lessons from the Pandemic. The report stated, "To survive future pandemics or catastrophic cyber incidents, the nation needs secure, remote access to reliable cloud services." The Committee on Oversight and Reform held a hearing on Wednesday, July 15 to discuss the next steps.

Throughout the years, there have been many cyberattacks in schools. In 2015, Florida students were unable to access state tests because hackers outside the U.S. were disrupting the system. A Missouri school district's cybersecurity was deemed underprepared in 2016 after the state audited its cyber safety measures. And just a few months ago, a survey found district leaders underestimate the depths of cybersecurity risks.

Cyberattacks on schools come in many forms, including breaches of student and educator data, identity theft, and money theft through business email compromises, according to Doug Levin, president of EdTech Strategies.

Along with introducing students to cybersecurity careers, the PROTECT Act could also teach students about proper cyber hygiene practices, such as how to create strong passwords and how to avoid phishing emails, Levin said.

"It's critical that students receive continuing and ongoing education on basic cyber hygiene practices," Levin said. "There is no good place for students to get reliable and trustworthy information on how to keep themselves secure. Schools are a very logical place to do this,

particularly as schools themselves are reliant on technology more and more to interact with students."

Interconnected IT Systems

The federal government has a responsibility to lead cyber protection efforts, because it encourages schools to adopt new technologies, Levin said. Plus, schools are online gateways into other local, state, and federal government agencies.

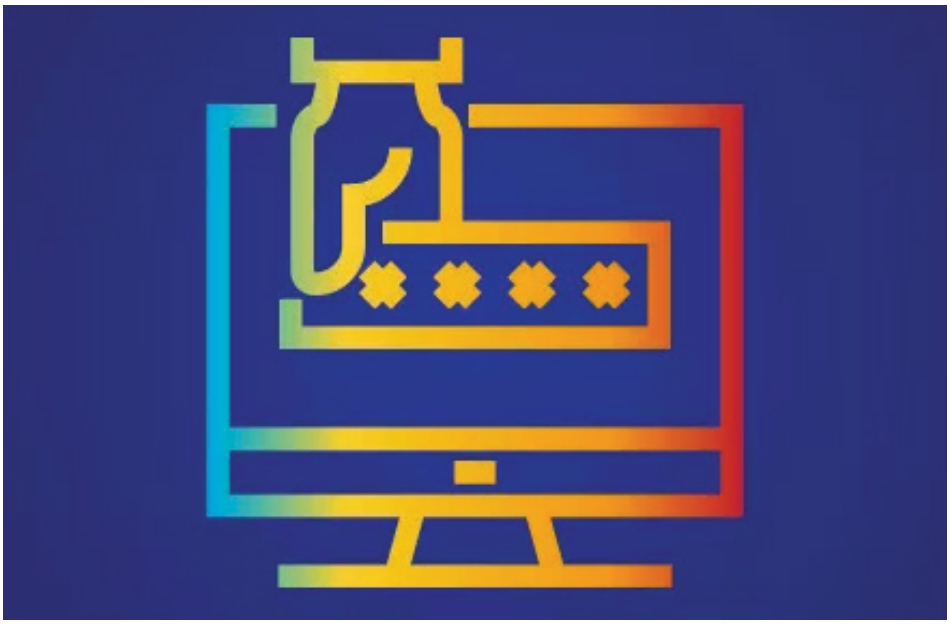
"School district IT systems are interconnected with other local state and federal systems, including voting systems, law enforcement, systems that have to do with employment and commerce," Levin said.

A national cybersecurity director would help connect schools so they could share information about cybersecurity challenges they are facing. "When something happens in a school district, other school districts around the country may or may not ever hear about what happened," Levin said. ■

Published on March 17, 2020, in Education Week's Special Report: Cyberattacks On Schools: How Educators Are Responding

Coronavirus Compounds K-12 Cybersecurity Problems: 5 Areas to Watch

By Jake Maher



—Getty

Cybersecurity experts have warned about coronavirus pandemic-related phishing scams targeting all sectors of the economy, from health care and consumer products to banking. Now, schools are being warned to be extra vigilant too.

Doug Levin, the founder and president of the K-12 Cybersecurity Resource Center, pointed out that schools have long been the subject of "drive-by" phishing scams: mass blasts of dubious emails looking to gather personal information. In recent years, they've also been hit with more sophisticated and targeted attacks.

The coronavirus pandemic, Levin said, compounds the problem.

"Scammers and criminals really understand the human psyche and the desire for people to get more information and to feel in some cases, I think it's fair to say in terms of coronavirus, some level of panic," he said. "That makes people more likely to suspend judgment for messages that might otherwise be suspicious, and more likely to click on a document because it sounds urgent and important and relevant to them, even if they weren't expecting it."

Here are 5 takeaways from a recent conversation Education Week had with Levin.

1. Remote Classes Can Make Schools More Susceptible

Moving to remote classes is an important step in promoting social distancing in order to limit the coronavirus' spread, but having students and teachers access schools' networks remotely also increases the potential for an attack, according to Levin.

"With more teachers and students online, particularly if they're doing it from less controlled environments outside of the school, the attack surface of the school community is increased," he said.

"In many cases, all it takes is for one person to make a mistake in a school community for a school district network to get infected, or a data breach to happen."

2. Don't Count on the Same Level of IT Support as Usual

Another challenge of a large number of students and teachers working remotely is that the increasing number of IT problems associated with e-learning will divert resources away from cybersecurity. Schools, Levin said, also tend to have older IT infrastructures, and staff that may not be as highly trained in cybersecurity as people in industries such as banking and healthcare.

If IT staff members have to work remotely, and maybe also have to deal with a flood of low-level tech support issues, they are going to be able to be less attentive to incidents as they start to emerge, according to Levin.

Hackers often pick chaotic times or moments when schools' defenses are down, like spring break or the time right before school starts, to attack, Levin added. The coronavirus pandemic is a large enough social disruption to attract that kind of attention.

3. Even Small Schools Aren't Safe

A common misconception, Levin emphasized, is that smaller schools are safer because

hackers don't think it's worth their time to target districts with only a few students.

"Based on the evidence I've seen about school cybersecurity events, the criminals and the scammers absolutely don't care who you are, where you are," Levin said. "It is just as easy to send an email to a rural small school as it is to a large bank."

4. Be Careful With Suspicious-Looking Links

In the days and weeks ahead, Levin said, schools need to redouble their precautions against opening suspicious links and email attachments from unknown or dubious addresses.

"School districts would do well to warn and build awareness, among both students and teachers, to have a little bit of skepticism when they are getting information appearing in their inboxes related to coronavirus, just to double-check who it is being sent from, whether this was an email they were expecting," Levin said. "If it's from an email address they don't recognize or normally don't get messages from, I think it's important to double check that email address."

He added that if teachers or students think they're receiving phishing emails, they should reach out to their IT staff to report it immediately.

5. Schools That Already Practice Good Cybersecurity Should Be Safe

Levin emphasized that for schools that are already on the lookout for cybercrime, their preventative measures should be enough.

"This is a time when schools would do well to be extra vigilant," he said. "But the good news is these sorts of incidents [can be prevented] if there are good cybersecurity practices in place already."

The coronavirus pandemic and the phishing scams that come in its wake should be a reminder, Levin said, that cybersecurity "needs to be a part of schools' continuity plan." ■

—Getty

Published on March 17, 2020, in Education Week's Special Report: Cyberattacks On Schools: How Educators Are Responding

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.**

A little more than a year ago, 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 instructional 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 last year 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 March 17, 2020, in Education Week's Special Report: Cyberattacks On Schools: How Educators Are Responding

Cyberattacks Force Schools to Bolster Online Security

By Alyson Klein

—Getty

The notification came in at 5:30 a.m. that something was wrong with the servers in the Cherry Hill School District outside Philadelphia. By 7:30, Wi-Fi was down. Email too.

Superintendent Joseph Meloche and his team later learned that a hacker had taken over their system, potentially through a phishing email. It took district officials and a slew of vendors more than two weeks to get everything back up and running, from staff email to the checkout system used in the school libraries. That meant 20-hour days, with emails flying back and forth daily from 5:30 a.m. to midnight.

And although learning was uninterrupted, the experience last fall was more than just

How Wichita Public Schools are using the Microsoft ecosystem to thrive in difficult times

Customer
Wichita Public Schools

Products and Services
Azure
Microsoft 365
Microsoft Teams
Power Automate
Power BI
Surface Go
Surface Go 2
Surface Pro
Surface Pro 7
Windows 10

Industry
K-12

Organization Size
Corporate (10,000+ employees)

Country
United States

November 12, 2020

For 150 years, Wichita Public Schools has provided its students with the skills and experiences they need to succeed in their careers and support their communities. This year is no different, although the district has had its share of added challenges. Like the students in many school districts, Wichita students went home for spring break in March 2020 and never returned to the classroom, upending the more established ways of educating. As Wendy Johnson, the Division Director of Strategic Communications for the Wichita Public Schools explains, "I find so much irony in the fact that we are celebrating 150 years of public education by totally reinventing a whole lot of we have been doing for so long."

As was the case elsewhere, Wichita's teachers were asked to generate new lesson plans for remote learning and IT professionals were asked to design solutions for problems with devices, connectivity, and access. Wichita's commitment to strategic planning, including investing in Microsoft's educational technologies, helped the district navigate the pandemic and help avoid the many challenging scenarios that have hampered other educational organizations worldwide.

In Wendy's view, "We have benefited greatly from a strategic plan because it set a clear vision for us to follow despite the uncertainty of the moment."

As was the case elsewhere, Wichita's teachers were asked to generate new lesson plans for remote learning and IT professionals were asked to design solutions for problems with devices, connectivity, and access. Wichita's commitment to strategic planning, including investing in Microsoft's educational technologies, helped the district navigate the pandemic and help avoid the many challenging scenarios that have hampered other educational organizations worldwide. In Wendy's view, "We have benefited greatly from a strategic plan because it set a clear vision for us to follow despite the uncertainty of the moment."

From devices to software: How investing in a cohesive ecosystem has paid dividends in a crisis

Rob Dickson is the CIO for the Wichita Public School system, and he credits much of Wichita's success to the technology decisions made before the pandemic. He explains, "I think there's a huge efficiency of having the manufacturer of the hardware and the manufacturer of the solution be the same company. You have to think about that holistic ecosystem."

Prior to Rob's arrival, the district's approach to technology looked a bit different. There was a noticeable digital divide among the students, teachers had not received professional development on existing technology, and there was a strong sense of skepticism regarding the cloud. As Rob notes, "I would say from my 30,000-foot view, coming into the district, the mindset here was very much still on-premises, a very much old-school way of thinking internal protected network versus this notion of trusting the cloud."

Rob began by adopting Microsoft 365 and pushing to use Microsoft Azure for key resources. Then, after reviewing the existing device inventory, he and his team began planning for device obsolescence with the added goal of getting to a 1:1 device model within a year and half. Rob's group then implemented Surface Pro 7 as the standard device for all faculty and staff, and the Surface Go 2 with LTE and HP devices for students at the new virtual school, Education Imagine Academy. As he explains, "What is nice about a Surface Pro is that it's a modern computing device. The teacher has a case that they can hold easily with their hand, and they can do classroom management while walking and assisting."

With resources in the cloud and device standardization underway, Rob was working on integrating much of the rest of the Microsoft 365 ecosystem when the pandemic struck. The transition required quick thinking and fast action. Rather than focusing on how to help students in a controlled classroom environment, he reflects, "If we have 50,000 kids in a remote environment, how do I support 50,000 different environments? So, you just basically turn the model inside out."

According to Rob, the district started by provisioning resources outside the network with tools. As he notes, "All of our apps are now provisioned via Azure proxy services. And we couldn't have done [it] in the old system because our VPN agents would not have been able to support it when we went remote. Had we not been able to just pivot very quickly, everything would have come to a halt—because we just wouldn't have been able to supply people with the right resources."

With new strategies for pivoting resources in place, Dickson turned to devices. By the end of October 2020, Wichita Public Schools will have 49,000 student devices and 6,000 additional devices for faculty and staff. Rob used the Windows 10 Out of Box Experience and Microsoft Intune for Education to deploy the first 32,000 devices

in five days. As Rob observes, “We take the devices that arrive and automatically hash them into Intune. From there, a student simply logs in with their school district account. Based upon the hardware hash and user account, their apps then automatically provision to the device.”

The benefits of this approach have become apparent as the school can customize the devices for individual student needs. “We provisioned CTE curriculum with software that was specific to a class,” Rob explains. “Because those containers are synced with our student information system, I can now designate software based upon a class that a student's taking that semester. We had never deployed software like this before, because everything was on-premises. And now, we are customizing the student experience while the students are still at home.”

Fostering innovation and collaboration with Microsoft Teams, Power Apps, Power Automate, and Power BI

As has been the case for many school districts around the world, the constraints imposed by remote learning have been key motivators for developing new and innovative approaches to education. In Wichita, the demand for remote learning led to a dramatic need for communication tools and efficient methods of decision making with a primacy on ways of looking at data to gauge the strengths and weaknesses of the new policies and procedures.

Microsoft Teams was introduced as a district-wide tool in late 2019, but the switch to remote learning propelled Teams to the forefront of the district’s strategy for handling the crisis. According to Rob, Teams became a crucial digital hub that integrated and synced a wide variety of data for educators while also acting as the primary tool for all meetings, and soon be used to link grades to student data. In Rob’s estimation, “Thankfully we had the ecosystem set because Teams became the default for how we did things.”

Although Teams has been instrumental for administrators and teachers, Rob points out that it has also been transformative for the students. “We now get to teach kids how to have a social, regular conversations in an environment that they are used to,” he explains. “In Teams, I can now teach that level of digital literacy to show how to have a meaningful conversation in a classroom setting that is very much a replication of what they do every day in the hundreds of thousands of apps that they use to communicate with each other.” With the help of Teams, Wichita Public Schools has been able to leverage its ecosystem to foster new and exciting 21st century learning techniques that benefit administrators, teachers, and students.

To facilitate collaboration and innovation within the ecosystem, the district has also taken advantage of Microsoft Power Automate and Power Apps to streamline automation and creation of new apps. “One of the things that we realized in the old paper-based process was that we weren't giving timely feedback if something was approved or not approved,” Rob notes. “In the new ecosystem, people get feedback every time as an app is either accepted or declined. Approved items then go out to a Power BI dashboard, and then anyone can go to that dashboard and see by grade level or by content area what apps are approved for what instructional purpose.”

Microsoft Power BI is not only useful for helping teachers understand what apps are available, but the district has also used Power BI to monitor student success—including everything from attendance to classroom activities. According to Wendy, “As a Power BI user, I'm finally able to answer my own questions. It provides a great deal of flexibility, which gives me an ability to understand stories and understand what data is telling us—not hysterics on social media or anecdotal examples. I want the data to power the stories, and that's been really enlightening to be able to see that and have that flexibility as we have moved through.”

Focusing on the mission: How students benefit from the strategic plan and cohesive Microsoft ecosystem

Wichita Public Schools has truly embraced the Microsoft ecosystem to empower its stakeholders to find ways for students and educators to thrive under incredibly challenging circumstances. "We are the largest single producer of new workforce every year in our community," notes Wendy. "And our community really looks to us to collaborate and support community needs for workforce." When the district shifted to remote work and learning, its strategic plan became an essential organizing framework for making sure that students were prioritized during the tumultuous period of transition. The district's commitment to using the entire Microsoft ecosystem—from devices to the various Microsoft 365 tools—has helped district leaders to facilitate innovation and collaboration where other districts have struggled.

The key, according to Rob, is that the district was already in a position to utilize the Microsoft ecosystem to develop rapid responses to the transition to remote learning without asking teachers to sacrifice the goals for their students. As he concludes, "With the Microsoft ecosystem, I can think about a holistic approach to having a collaborative space where everyone is contributing. We constantly think about all the things that go into a face-to-face classroom environment, and now that we have these tools, we can work to replicate those functions in a remote learning environment."

For administrators, educators, parents, and students, that means that the Wichita Public School district is in a position to mark its 150-year anniversary with the full confidence that the community is well-positioned to continue to succeed, no matter what challenges lie ahead. The stakes couldn't be higher. As Wendy notes, "We have 50,000 students, and they have one chance to get it right on any given day or any given school year. What is at stake is whether our kids will get the best possible education that we can offer them."

View the story online at:
https://customers.microsoft.com/en-us/story/853660-wichita-public-schools-education-azure-en-united-states

a technical nightmare, Meloche said. The district had to explain to parents why they were unable to email their child's teacher.

"It seemed like, 'Wow, the district is falling apart,' but we were actually functioning and functioning well," said Farrah Mahan, Cherry Hill's curriculum director. Still, the task of getting back to normal was grueling. "This was a marathon, you have to be slow and steady and pace yourself. There was a lot of conversation about self-care and making sure that we were taking some moments to be offline."

Cherry Hill is far from alone. There have been at least 775 publicly disclosed cyber incidents nationally since 2016. That includes phishing attacks, data breaches, ransomware attacks, and denial-of-service attacks, according to the K-12 Cybersecurity Resource Center. And the number of incidents more than doubled in 2019, compared with 2018, from 122 to 348.

In fact, 2019 had the highest number of incidents since Douglas Levin, the founder and president of EdTech Strategies, began tracking the problem.

One possible explanation: School hacks are increasing because K-12 school systems are so reliant on technology and have potentially valuable data on students and employees, Levin said. "There are bad guys who are targeting [schools] because they've become successful," Levin said.

He added that the coronavirus pandemic could exacerbate the problem because hackers play on people's fears, more students could be using school-issued devices at home more often, and dealing with coronavirus-related technology needs could divert IT resources away from cybersecurity efforts.

Serious Consequences

Some systems, including Alabama's Houston County school district, have had to close or postpone classes. The Rockville Center School District outside New York City paid hackers $100,000 to recover its data, according to local news reports. (The payment was covered by the district's insurance policy, the local radio station reported.) Back in September, Louisiana Gov. John Bel Edwards, a Democrat, declared a statewide emergency after school systems in three parishes were hit by cyberattacks.

Districts are coping mostly with ransomware attacks, which will encrypt files in a computer and can quickly render entire systems inaccessible, and phishing attacks, which seek to steal employee credentials so that hackers can get into a computer system or steal valuable data, said Amy McLaughlin, the cybersecurity director for the Consortium for School Networking.

These tactics aren't always sophisticated. The classic phishing attack could be an email that says something like "this is an emergency, please send all W-2 forms for current employees," McLaughlin said. Or a hacker may try to copy the email of a district leader, say the superintendent, and ask their executive team to buy gift-certificates and send the codes to them right away.

K-12 systems make "really easy targets" because they are staffed by helpful, diligent people, and because district leaders' schedules are a matter of public record, so it would be easy for a hacker to include seemingly relevant details in a phishing email, McLaughlin said.

'Cybersafety' Is Key Word

McLaughlin's number one piece of advice for combatting those types of scams? Train staff. And she's not talking about a quick, 15-minute annual in-service training, sandwiched between other professional development. She'd rather see "an ongoing marketing campaign" where everyone in the district reminds staff, and even students, to report phishing scams. Districts could offer a reward each month for the person who reports the most potential problems, she suggested, or have students make posters about the problem.

Staff should be encouraged to report every possible attempt. District tech leaders "would much rather spend time saying, 'nope that's not legit,' than to have someone click [on a suspicious link or email] even once."

She also suggests districts use the term "cybersafety" when discussing these issues. "When you talk about safety, people listen," she explained. "When you talk about cybersecurity, it sounds like some nerdy, geeky thing and their eyes glaze over."

Reporting every possible hacking attempt is advice Cherry Hill took after the hack earlier this year. After the incident, district leadership also moved email to a cloud-based system, with two-factor authentication. And officials told employees, "If you receive an email from an external person, if you don't recognize the person or the name, don't click on any forms," Mahan said. "One person in a district of 11,000 could bring down our entire system. You have to be mindful of what you're clicking on."

But not every district trains its employees on cybersecurity. In fact, in a survey conducted by CoSn and Education Week, 44 percent of CTOs said they don't offer such training. Another 35 percent said they offer training to both teachers and principals. And nearly 18 percent said they planned to add training this school year.

> "If you receive an email from an external person, if you don't recognize the person or the name, don't click on any forms. One person in a district of 11,000 could bring down our entire system. You have to be mindful of what you're clicking on."
>
> **FARRAH MAHAN**
> CHERRY HILL'S CURRICULUM DIRECTOR

Back Up Computer Systems

Districts also need to do some technical work, including backing up their systems, and testing those backups. "A lot of ransomware attacks are successful because backups have been compromised," McLaughlin said. Staff should make sure they are storing files in a place where it can be backed up, not directly on their laptops.

Jason Dial, the superintendent of the Ava R1 school district, in southwestern Missouri, which experienced an attack earlier this school year, seconded that advice.

"Be sure that you have quality backup solutions," he said. "If it hasn't happened to you yet, it's going to happen. In order to be ready for it, you have to make sure you have prepared yourself so that you're not down very long." His district, he said, had recently installed backups and "didn't lose anything" but "if it had happened to us a year ago, we would have been in a lot worse situation."

Many districts are already working on backups, according to the CoSn/Education Week survey of 513 K-12 technology leaders in the United States Seventy-three percent of education technology leaders suggested they were backing up all information and storing it off site in case of an attack. Other popular

strategies included encouraging staff to upgrade passwords (69 percent), increasing use of encryption (47 percent), having cybersecurity practices audited by an outside organization (34 percent), and convening a cybersecurity team (20 percent).

Sometimes, hackers demand a ransom for restoring a district's data. McLaughlin's advice: Don't pony up. "I would certainly recommend against paying, because it's just like kidnapping," she said. "People will continue to do that if they continue to get rewarded."

Dial said that when district officials arrived at school on the day of the hack, several printers had messages on them saying "we have locked all of your data. If you would like it back, please send an email to this email address and we will send further instructions."

But the hackers never heard from the Missouri district. "We choose not to respond to those types of threats. We knew that we had quality backup solutions off site," Dial said.

And, in case the worst happens, McLaughlin recommends districts have a cyber security plan in place that's been read and vetted by lawyers. Key staff should know what they need to do and what sort of information they need to have, in the event that they have to call the insurance company.

District leaders also need to make sure they have an incident response plan in the event of a cyber event—and they should practice it, just like they would a fire drill, McLaughlin said. "Having that pre-prepped is so much better than trying to build an airplane while you're flying it," she explained.

Another piece of wisdom from district leaders who have weathered attacks: Be sure to put some money aside in case the worst happens. Bob Blalock, the technology coordinator in Houston County, said his district might have ended up in a tight financial spot without some funding in reserves.

"We were very fortunate we had some budget for an emergency situation," he said. "We are not an affluent school system." (Blalock declined to say just how much the district spent rectifying the situation other than that it was "very expensive.") ■

Intern Jake Maher contributed to this article.

—Getty

OPINION

Published March 19,2019, in Education Week's Special Report: K-12 Cybersecurity: Big Threats And Best Practices

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 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.

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.

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.

— Getty

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.

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