Hackers prey on public schools, adding stress amid pandemic

January 31 2022, by Cedar Attanasio

Art teacher Sarah Hager works at a computer in her classroom at Cleveland Middle School on Sunday, Jan. 23, 2022, in Albuquerque, N.M. Public school systems – which often have limited budgets and cybersecurity expertise—have become an inviting target for ransomware gangs. The coronavirus pandemic has forced schools to turn increasingly toward virtual learning, making them more dependent on technology and more vulnerable to cyber-extortion. Credit: AP Photo/Cedar Attanasio

For teachers at a middle school in New Mexico's largest city, the first inkling of a widespread tech problem came during an early morning staff call.

On the video, there were shout-outs for a new custodian for his hard work, and the typical announcements from administrators and the union rep. But in the chat, there were hints of a looming crisis. Nobody could open attendance records, and everyone was locked out of class rosters and grades.

Albuquerque administrators later confirmed the outage that blocked access to the district's student database—which also includes emergency contacts and lists of which adults are authorized to pick up which children—was due to a ransomware attack.

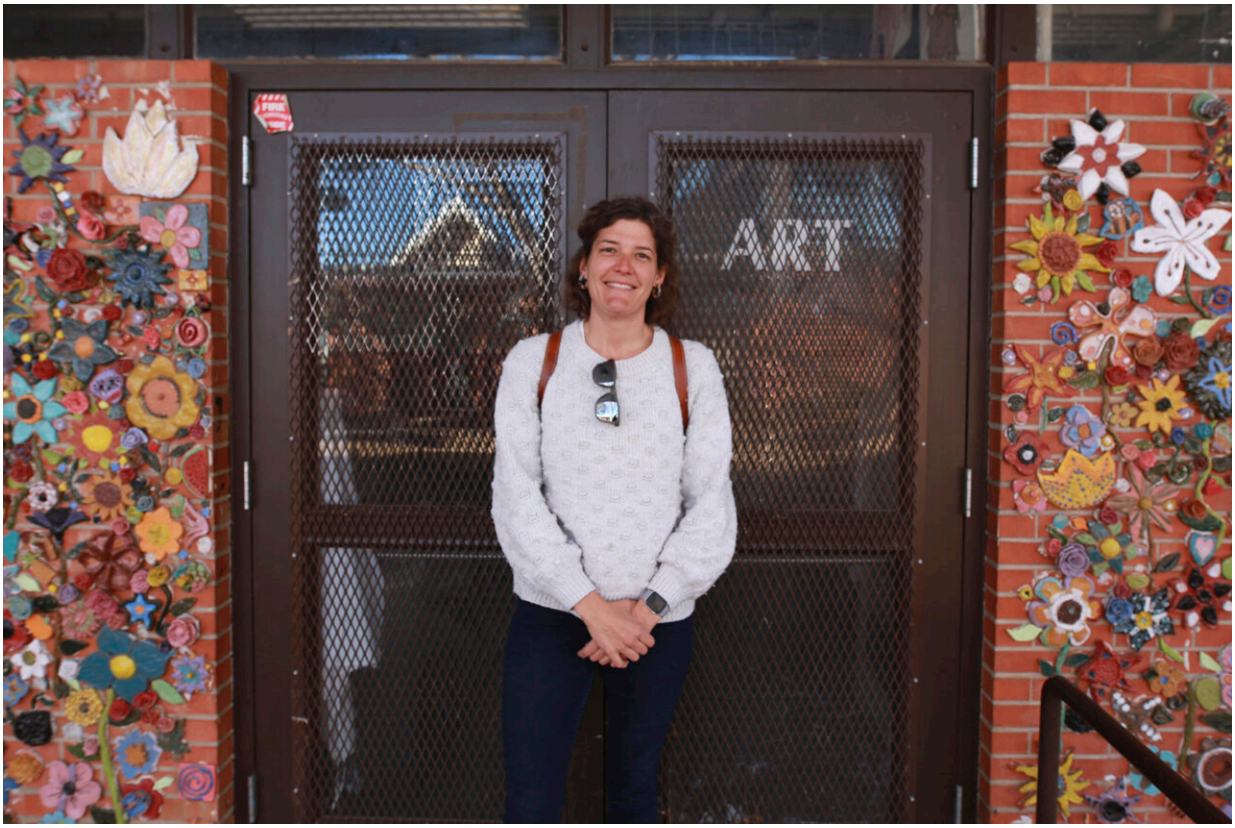
"I didn't realize how important it was until I couldn't use it," said Sarah Hager, a Cleveland Middle School art teacher.

Cyberattacks like the one that canceled classes for two days in Albuquerque's biggest school district have become a growing threat to U.S. schools, with several high-profile incidents reported since last year. And the coronavirus pandemic has compounded their effects: More money has been demanded, and more schools have had to shut down as they scramble to recover data or even manually wipe all laptops.

"Pretty much any way that you cut it, incidents have both been growing more frequent and more significant," said Doug Levin, director of the K12 Security Information Exchange, a Virginia-based nonprofit that helps schools defend against cybersecurity risk.

Precise data is hard to come by since most schools are not required to publicly report cyberattacks. But experts say public school systems—which often have limited budgets for cybersecurity

expertise—have become an inviting target for ransomware gangs.



Art teacher Sarah Hager poses outside her classroom at Cleveland Middle School on Sunday, Jan. 23, 2022, in Albuquerque, N.M. Public school systems – which often have limited budgets and cybersecurity expertise—have become an inviting target for ransomware gangs. The coronavirus pandemic has forced schools to turn increasingly toward virtual learning, making them more dependent on technology and more vulnerable to cyber-extortion. Credit: AP Photo/Cedar Attanasio

The pandemic also has forced schools to turn increasingly toward virtual learning, making them more dependent on technology and more vulnerable to cyber-extortion. School systems that have had instruction

disrupted include those in Baltimore County and Miami-Dade County, along with districts in New Jersey, Wisconsin and elsewhere.

Levin's group has tracked well over 1,200 cyber security incidents since 2016 at public school districts across the country. They included 209 ransomware attacks, when hackers lock data up and charge to unlock it; 53 "denial of service" attacks, where attackers sabotage or slow a network by faking server requests; 156 "Zoombombing" incidents, where an unauthorized person intrudes on a video call; and more than 110 phishing attacks, where a deceptive message tricks a user to let a hacker into their network.

Recent attacks also come as schools grapple with multiple other challenges related to the pandemic. Teachers get sick, and there aren't substitutes to cover them. Where there are strict virus testing protocols, there aren't always tests or people to give them.

In New York City, an attack this month on third-party software vendor Illuminate Education didn't result in canceled classes, but teachers across the city couldn't access grades. Local media reported the outage added to stress for educators already juggling instruction with enforcing COVID-19 protocols and covering for colleagues who were sick or in quarantine.

Albuquerque Superintendent Scott Elder said getting all students and staff online during the pandemic created additional avenues for hackers to access the district's system. He cited that as a factor in the Jan. 12 ransomware attack that canceled classes for some 75,000 students.

The cancellations—which Elder called "cyber snow days"—gave technicians a five-day window to reset the databases over a holiday weekend.

Elder said there's no evidence student information was obtained by hackers. He declined to say whether the district paid a ransom but noted there would be a "public process" if it did.

The Cleveland Middle School, that was impacted by a recent cyberattack, is shown on Jan. 23, 2022, in Albuquerque, N.M. Cybersecurity experts say that ransomware attacks on K-12 schools have increased during the pandemic. Cyberattacks like the one that canceled classes for two days in Albuquerque's biggest school district have become a growing threat to U.S. schools, with several high-profile incidents reported since last year. Credit: AP Photo/Cedar Attanasio

Hager, the art teacher, said the cyberattack increased stress on campus in ways that parents didn't see.

Fire drills were canceled because fire alarms didn't work. Intercoms stopped working.

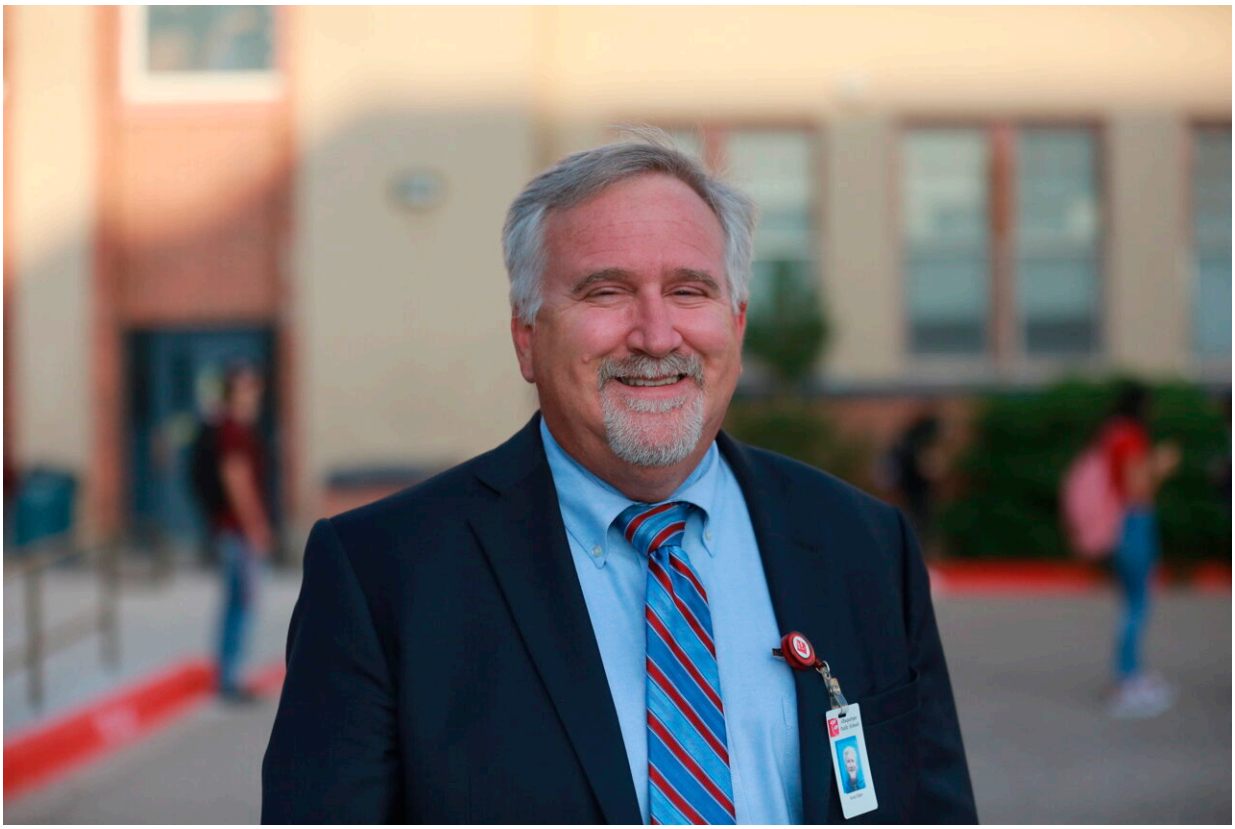
Nurses couldn't find which kids were where as positive test results came in, Hager said. "So potentially there were students on campus that probably were sick." It also appears the hack permanently wiped out a few days worth of attendance records and grades.

Edupoint, the vendor for Albuquerque's student information database, called Synergy, declined to comment.

Many schools choose to keep attacks under wraps or release minimal information to prevent revealing additional weaknesses in their security systems.

"It's very difficult for the school districts to learn from each other, because they're really not supposed to talk to each other about it because you might share vulnerabilities," Elder said.

Last year, the FBI issued a warning about a group called PYSA, or "Protect Your System, Amigo," saying it was seeing an increase in attacks by the group on schools, colleges and seminaries. Other ransomware gangs include Conti, which last year demanded $40 million from Broward County Public Schools, one of the nation's largest.



Albuquerque Public Schools superintendent Scott Elder poses for a photo outside of Highland High School on Aug. 11, 2021, in Albuquerque, N.M. Cybersecurity experts say that ransomware attacks on K-12 schools have increased during the pandemic. Elder said getting all students and staff online during the pandemic created additional avenues for hackers to access the district's system. He cited that as a factor in the Jan. 12, 2022, cyberattack that canceled classes for some 75,000 students. Credit: AP Photo/Cedar Attanasio, File

Most are Russian-speaking groups that are based in Eastern Europe and enjoy safe harbor from tolerant governments. Some will post files on the dark web, including highly sensitive information, if they don't get paid.

While attacks on larger districts garner more headlines, ransomware gangs tended to target smaller school districts in 2021 than in 2020,

according to Brett Callow, a threat analyst at the firm Emsisoft. He said that could indicate bigger districts are increasing their spending on cybersecurity while smaller districts, which have less money, remain more vulnerable.

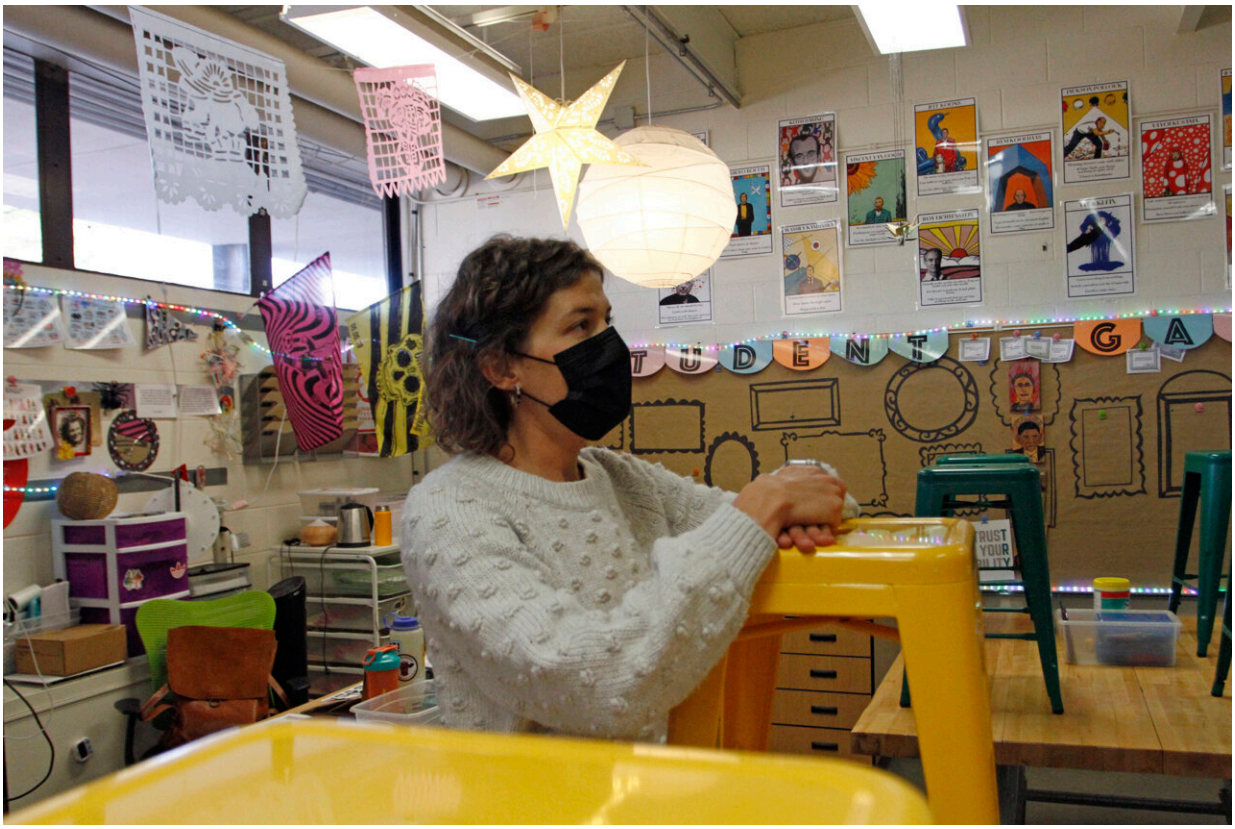
A few days after Christmas, the 1,285-student district of Truth or Consequences, south of Albuquerque, had its student information system shut down by a ransomware attack. Officials there compared it to having their house robbed.

"It's just that feeling of helplessness, of confusion as to why somebody would do something like this because at the end of the day, it's taking away from our kids. And to me that's just a disgusting way to try to, to get money," Superintendent Channell Segura said.

The school didn't have to cancel classes because the attack happened on break, but the network remains down, including keyless entry locks on school building doors. Teachers are still carrying around the physical keys they had to track down at the start of the year, Segura said.

In October, President Joe Biden signed the K-12 Cybersecurity Act, which calls for the federal cyber security agency to make recommendations about how to help school systems better protect themselves.

New Mexico lawmakers have been slow to expand internet usage in the state, let alone support schools on cyber security. Last week, state representatives introduced a bill that would allocate $45 million to the state education department to build a cybersecurity program by 2027.



Art teacher Sarah Hager poses in her classroom at Cleveland Middle School on Sunday, Jan. 23, 2022, in Albuquerque, N.M. Public school systems – which often have limited budgets and cybersecurity expertise—have become an inviting target for ransomware gangs. The coronavirus pandemic has forced schools to turn increasingly toward virtual learning, making them more dependent on technology and more vulnerable to cyber-extortion. Credit: AP Photo/Cedar Attanasio

Ideas on how to prevent future hacks and recover from existing ones usually require more work from teachers.

In the days following the Albuquerque attack, parents argued on Facebook over why schools couldn't simply switch to pen and paper for things like attendance and grades.

Hager said she even heard the criticism from her mother, a retired school teacher.

"I said, 'Mom, you can only take attendance on paper if you have printed out your roster to begin with,'" Hager said.

Teachers could also keep duplicate paper copies of all records—but that would double the clerical work that already bogs them down.

In an era where administrators increasingly require teachers to record everything digitally, Hager says, "these systems should work."

—

This version has been updated to correct that Truth or Consequence does not use the software product Synergy.