TechXplore

# Student information remains at risk after massive cyberattack on Los Angeles Unified

September 7 2022, by Howard Blume and Alejandra Reyes-Velarde

Credit: Pixabay/CC0 Public Domain

The private data of more than 400,000 students could be at risk as federal and local investigators assess the damage wreaked by a massive cyberattack against the Los Angeles Unified School District, which overcame a complete digital shutdown to open schools on schedule Tuesday.

The district did not know whether student information—assessments, grades, class schedules, disciplinary records, reports about disabilities—was accessed by hackers through the district's online student management system.

"We're still going through student files because ... the student management system was touched," Supt. Alberto Carvalho said at a downtown news conference, accompanied by Los Angeles Mayor Eric Garcetti and Los Angeles Police Chief Michel Moore. He said the hackers have encryption skills to cover their tracks and "shut us out of what they have or what they saw."

"We have not seen evidence of health information being accessed or Social Security numbers for students being accessed," Carvalho said. The payroll system too, he added, is functioning, and personnel data do not appear to have been compromised. "But any type of access is one that concerns us."

Underscoring the seriousness of the attack on the nation's second-largest school district, an investigation involving the FBI, the Department of Homeland Security and local law enforcement is underway. Carvalho said the attack, discovered Saturday at 10:30 p.m., was launched by a "ransomware tool that temporarily disabled systems, froze others and had access to some degree of data."

There are indications that the hack could have originated in a foreign country, and Carvalho said there has not been a ransom demand.

"I'm not going to get into much detail, but there are three nations that investigators have traced some degree of trail to," Carvalho said. "But that doesn't necessarily indicate that's where the attack came from."

District staff recognized the breach quickly and took fast action that may have averted an operational disaster.

If the district had lost the ability to manage its fleet of buses, "over 40,000 of our students would not have been able to get to school," Carvalho said. If food services or payroll systems had been taken down, the impact "would have been significant, very disruptive and debilitating to our school system."

District officials may have thwarted the worse outcome by taking the unprecedented move of shutting down all district systems. But recovering from the shutdown created problems of its own—assignments and lesson plans were inaccessible over the weekend. And no student or employee had access to the system until they were able to reset their password, a process that began about 9 a.m. Tuesday, with school already in session. The resets were not completed by the end of the school day.

School districts are vulnerable targets for various reasons, including a preference for using funding for needs other than cybersecurity, and because online systems have to provide for public access. For 2021, cybersecurity firm Emsisoft, which tracks cyberattacks in education and other sectors, tallied 88 educational organizations affected by ransomware: 62 school districts and 26 colleges and universities.

A notable local attack targeted the Newhall school system in 2020. In May, the Chicago public school system announced that a massive data breach exposed four years' worth of records of nearly 500,000 students and just under 60,000 employees.

A recent cyberattack targeted a company, Illuminate Education, whose clients include L.A. Unified and whose services, according to its website, reach "more than 17 million students" in 5,200 schools and school districts.

L.A. officials said Monday there is no apparent link between the ransomware attack and the Illuminate breach.

What makes LAUSD "an attractive target" is the number of individuals affected when district systems become unavailable, said Clifford Neuman, director of the USC Center for Computer Systems Security. "This makes the impacted organization potentially more willing to pay a ransom to recover their systems, and encourages criminals to seek larger payments."

The hackers can demand ransoms both to restore systems and to keep private data from being posted publicly, as has happened with the Clark County School District in Nevada.

Cybersecurity expert Brett Callow said it's "entirely possible" that fast action by L.A. Unified helped enormously.

"Organizations sometimes realize they have a problem when systems start to be encrypted," said Callow, a threat analyst for Emsisoft.

"Encryption is usually the last step in an attack, though," he added. In other words, a massive amount of data could already have been stolen by the time the district stepped in to prevent an operational meltdown.

By late Sunday night, officials determined that the most vital systems were usable, and Carvalho decided to open schools as scheduled Tuesday.

"No. 1, we are experiencing a fairly normal school day, and that was our intent," Carvalho said, speaking to reporters at the Roybal Learning Center.

But there were problems, especially early in the day.

"Some teachers are under the impression they can change their LAUSD password, then log in, but the password site is down," one teacher said.

"I am unable to do my job, which is to assure students are present in school," an attendance counselor reported. "We do have paper attendance we will be collecting, but I would usually call home or go on home visits to find out students' whereabouts. Unfortunately, with not having access to their information, I will not be able to find out where those students are."

Fourth-grade teacher Richard Powels was able to reset his password, but his students, who had to go through the process on campus, experienced a wait time of five minutes to access the reset website, then it wouldn't accept their credentials.

"Hopefully it will be better tomorrow," said Powels, who teaches in a magnet program at Clifford Street Elementary in Echo Park. As of Tuesday afternoon, "no students are able to use their devices at school. We've had to improvise with our plans a bit to make sure everyone is engaged and learning."

The district did not announce the attack until Monday night because, Carvalho said, a critical assessment and response was in progress and because the release of information had to be vetted through different agencies with a role in the investigation.

When the district acknowledged the attack, officials also announced an array of measures to improve cybersecurity. These measures, the district said, "have been taken, will be taken immediately or will be implemented as soon as feasible."

The list includes:

- Setting up an independent Information Technology Task Force. It would be charged with developing recommendations within 90 days and providing monthly updates.

- Deploying technical staff across the vast school system to assist with issues that arise in the coming days.
- Reorganizing departments and systems "to build coherence and bolster data safeguards."
- Appointing an expert technology advisory council and naming a technology advisor who will focus on security procedures and practices as well as an overall data center operations review.
- Adding budget dollars as needed and improving employee training.
- Analyzing systems with help from federal and state law enforcement.

Police Chief Moore said the risk from cyberattacks should not be underestimated. "It is the No. 1 threat to our safety, and it is an invisible foe and it is a tireless foe," Moore said. "It requires all of us to work together to work to identify these threats and these actors and to take steps to mitigate the damage.

"This is a wake-up call, a reminder," Moore added, "because all of us are so dependent on our cyber universe."

Garcetti said authorities are on alert for further attacks on city networks. He highlighted the challenge from hackers, saying that the city has to fend off 1 billion cyberattacks every month: "That's with a B," he said.

"We are all vulnerable to these attacks. If you're a small-business owner listening to this today, it's not just big entities like LAUSD," Garcetti said.

"It can be and has been small businesses. It's medium- and big-sized businesses. It's government agencies. It's nonprofits."

Distributed by Tribune Content Agency, LLC.

Citation: Student information remains at risk after massive cyberattack on Los Angeles Unified (2022, September 7) retrieved 27 April 2024 from https://techxplore.com/news/2022-09-student-massive-cyberattack-los-angeles.html