# Report identified key vulnerabilities two years before cyberattack on LA Unified

September 8 2022, by Howard Blume

Credit: CC0 Public Domain

An internal report identified key vulnerabilities in the data systems of the Los Angeles Unified School District two years before hackers launched a major cyberattack that has disrupted operations this week in

the nation's second-largest school system.

The report indicated that district staff agreed with its findings and committed to addressing them, but district officials did not clarify Wednesday which of the recommended actions were carried out.

The private data of more than 400,000 students could be at risk from the massive cyberattack that was identified late Saturday night. L.A. Unified overcame a complete digital shutdown to open schools on schedule Tuesday, but disruptions to normal learning and some business operations occurred across the vast school system throughout the day. Much of the district website remained inaccessible through Wednesday.

District officials said they did not know whether student information in the district's student management system—including assessments, grades, class schedules, disciplinary records and reports about disabilities—was accessed by the hackers. However, they said they believe that Social Security numbers, medical records and payroll information for employees remain secure.

The cybersecurity audit was published in September 2020 and conducted by outside consultants working with district technology staff under the supervision of the district inspector general's office.

The Times obtained a redacted version that was prepared for those without security clearance. Confidential portions, including most of 38 specific findings accompanied by 38 recommendations, are not included.

Even so, the report, in bureaucratic language, sounded an alarm. In spot testing, "auditors were able to gain access to certain sensitive information including a limited number of Social Security numbers," the report stated.

Auditors also were able to obtain LAUSD passwords and "able to convince employees to unknowingly execute malicious codes."

Numerous "high-risk" areas were identified, involving the structure of district systems, inadequate procedures and insufficient security training for employees.

Among the problems identified in 2020:

- The technology division did not have a process in place to make sure the organization was complying with security standards.
- The district lacked adequate "incident response training" to react, for example, to hacking or another emergency.
- Certain classes of computer accounts had substandard security.

On Tuesday, L.A. Unified Supt. Alberto Carvalho, who has been in charge since February, announced a long list of cybersecurity measures that are or would soon be in place.

The 2020 report contained a general description of the L.A. Unified system, noting that "security is provided via multiple, redundant firewalls with content filtering and intrusion detection system capabilities."

The main data center is housed in district headquarters on South Beaudry Avenue just west of downtown, occupying an entire floor. A backup site in Van Nuys serves "as a disaster recovery site."

The report was redacted out of concern over "highly sensitive information that could be leveraged by attackers targeting the district," the introduction stated.

The hack represents a major security failure, and it could be weeks before the district knows the extent of the harm or what private data was

extracted.

L.A. Unified is far from alone among school districts that have been targeted. Hackers have compromised confidential information in school systems serving Las Vegas, Chicago and New York City.

In L.A., a quick shutdown of district systems when the breach was discovered may have prevented much greater harm, Carvalho said Tuesday.

Emergency systems and the technological components of key operations—including food services and bus transportation—were functional, which gave Carvalho the confidence Monday night to decide to open schools on a normal schedule after the Labor Day holiday.

But it was not business as usual.

"The recovery from the disruption has proven more challenging than initially anticipated," officials acknowledged in a statement Wednesday afternoon.

A seventh-grade teacher said that Tuesday was challenging, with some teachers unable to reset online accounts until after school.

"Virtually everything we do during a school day depends on access to LAUSD accounts, even how the students sign out to use the bathroom during class," she said. Because of a delay in the arrival of textbooks, students had been using digital curriculum, much of which was temporarily out of reach.

And she reported an additional aggravation: "In order to troubleshoot and reset the public address system, there were frequent loud testing sounds spontaneously interrupting classes."

Parents were concerned about the disruptions too. "My son goes to Hamilton HS," Justin Kahn said via Twitter. "He said all classes were basically dead in the water, no access to any of the coursework, and to make the matter worse… Hamilton also didn't have working AC."

A civics teacher at one South L.A. school reported that the day was gloriously technology-free, resulting in one of the best instructional days ever.

But parent Elizabeth Hernandez couldn't help but worry. One of her children has a disability that requires an individualized education plan, for which she submitted extensive personal information.

"It's scary because we don't know exactly how much information is out there," Hernandez said. "Anyone can steal their identity."

Since the hack, her third-grader hasn't had major difficulties in class because most classroom activities at that level don't require computer access.

But her teenager was concerned about being shut out from his district account, which students use to receive, carry out and file assignments.

The reboot of district systems involved resetting hundreds of thousands passwords, which had to be done at a district site—except for some 7,000 students whose families opted this year for remote online learning.

Carvalho said those students would be helped via the technology hotline, but advised that there might be delays.

"Today was very chaotic and complicated," one virtual academy secondary student told The Times. She was able to get into her Zoom session, but most other students were locked out. She worried about

inaccessible schoolwork piling up, calling Tuesday "unproductive, stressful."

Wednesday, she said, was "completely the same" with teachers and students still struggling to change passwords.

"My homeroom/English teacher is also very lost and doesn't even know what to do," she said.

The student said she was on hold with the helpline for 32 minutes before she accidentally disconnected.

But by Wednesday, workarounds were being established: Teachers had students log in to the free online Khan Academy instead of their regular platform so they could tackle their math problems.

In a statement Wednesday, Carvalho thanked students and staff for their persistence and patience.

"We understand that this has been a frustrating and confusing experience for many," he said, "and our teams are working diligently to help our community regain access to all systems as quickly as possible."