LA Unified cyberattack woes and uncertainties could be long-lasting, experts say

October 11 2022, by Howard Blume, Alejandra Reyes-Velarde and Kiera Feldman

Credit: CC0 Public Domain

Retirees from the Baltimore school system are having trouble with pension and health care payments two years after a ransomware attack.

The identity of a child in Toledo, Ohio, is being used to apply for credit months after a cyberattack on schools there. A midsize Texas school district last year paid more than half a million dollars in ransom to restore access to its system and prevent the posting of sensitive data online.

The repercussions of an attack on vulnerable school systems can be strong, long-lasting and expensive, which is why cybersecurity experts warn against expecting a quick and clean resolution to the massive hack in September on the Los Angeles Unified School District.

Uncertainties over the stolen data will persist well into the future not only for the district but also for those whose personal information was published on the dark web, they said.

Although L.A. Superintendent Alberto Carvalho expressed confidence last week that the criminal syndicate behind the attack largely failed to steal valuable data, the implications and full extent of the breach remain difficult to know.

Education institutions have been increasingly targeted in recent years, in part because they have multiple public-facing portals and third-party applications accessible to students, parents and the community. And costly cybersecurity prevention has to compete with other pressing needs—becoming a financial and staffing burden for small districts and an extraordinarily complicated task for a behemoth such as L.A. Unified, which manages records for millions of current and former students, employees and contractors.

"Students are trusting the school district to keep their information safe and clearly they haven't managed to do so," said Runa Sandvik, a security researcher and founder of Granitt, a startup that focuses on security for journalists and at-risk people around the world.

Experts warn there is no reason to trust cybercriminals over how much data they said they stole. Also, the data could be exploited far into the future, in ways that are difficult to detect, let alone prevent.

"Unfortunately reversing a data breach is like putting toothpaste back in the tube," said Jeremy Kirk, executive editor for security and technology for Information Security Media Group.

The L.A. Unified attack was discovered on Saturday, Sept. 3, during the Labor Day weekend. Technicians quickly shut down computer systems to blunt the intrusion, although some disruptions continue more than a month later.

About half of the servers were encrypted in the facilities division—making them inaccessible. Still, district officials believe that the fast counteraction averted pervasive data theft. The school system refused to pay a ransom and, as a result, the hackers posted about 500 gigabytes of district data online.

The number of individuals with compromised personal data appears to be small—compared to the millions of people who have data held in district systems. However, officials were not prepared last week to say how many people are affected. That analysis is ongoing.

The data at stake in any school system attack would include names, addresses, dates of birth and Social Security numbers—a more serious matter than, say, an "ephemeral" hack on a building supply store that would yield names and credit card numbers, said John Childs, director of information security solutions for DynTek, a national information-technology consulting service based in Irvine.

L.A. Unified does not collect student Social Security numbers, and officials said no employee database that stored payroll, banking, Social

Security or medical information was accessed, but some contractors working in the facilities division were not so fortunate.

Even without Social Security numbers, internet operatives can begin to build a profile of an individual, even a child, that can be used fraudulently, sooner or later. The lost data did include date of birth and address for many students enrolled at some point from 2013 through 2016 and for some employees during that period.

Such victims might need to be "always looking over their back," said Childs, who has not analyzed the L.A. Unified breach. "It's not just a risk while authorities are focused on the breach."

Months after a recent data breach in the Toledo schools, the parents of an elementary student reported that someone had stolen their son's identity to apply for a car loan, a credit card and discounted utility rates.

The ripple effects include potential litigation against the school system for not safeguarding data. L.A. Unified could face similar risks, experts said.

Sandvik noted that L.A. Unified was warned of vulnerabilities in a 2020 internal audit: "What really stands out to me is that you have a school district that's been aware for quite some time of some deficiencies they have and has not addressed them."

District officials said they would try to reach those whose information was stolen and offer credit monitoring, although some experts said they were doubtful that credit monitoring would provide much value. Carvalho announced a series of measures to prevent future attacks, while acknowledging the district failed to act on major recommendations from the 2020 security audit.

Officials say they don't know how the hackers got in, but the remedies will include multifactor authentication, which typically requires more than one password. The district also will limit the use of outside apps that create a potential backdoor into the system.

A case in point is the data breach early this year at Illuminate, a company that provides education services. That breach affected school districts across the country, including L.A. Unified. More than 4,700 L.A. Unified students enrolled between 2008 and 2010 had personal data compromised, the district told a technology publication in response to a public-records act request. Illuminate sent out notices to those affected from L.A. Unified in May, according to state records.

Although the larger L.A. Unified hack in September was notable because of the size of the school system, some experts downplayed its magnitude.

"It's not great," said security technologist Bruce Schneier, about the hacking. "But in the scheme of things, don't make people terrified. This kind of nonsense happens all the time."

Hospitals have been "shut down" by cyberattacks, said Schneier, who writes the blog Schneier on Security "That feels bigger." A cyberattack last week on CommonSpirit Health, the nation's second-largest nonprofit hospital chain, forced "ambulance diversions, system shutdowns and patient appointment rescheduling," including for critical procedures, The Washington Post reported.

But for schools starved for resources, the attacks can be financially painful and difficult to manage.

A 2020 attack on the Baltimore schools has resulted in more than $8 million in costs, including $900,000 for the repair of the student

information system, $860,000 for investigation, $50,000 for public relations and $11,500 for ransomware negotiation services. Major problems persist with pension and health insurance payments for retirees. Some retirees were hit with collection notices for "underpaying" insurance premiums, one bill was for $20,000, even though they said they'd paid what the district required.

Carvalho said L.A. Unified's dollar cost to date is negligible—essentially employee overtime—because of pro bono services and help from other government agencies and law enforcement. But there will be significant costs moving forward to prevent another attack, he said.

The district also has cyberattack insurance, but whether it took proper preventive measures could affect the payment of a claim, experts said.

Cyberattack insurance has had some unintended consequences, said Brett Callow, threat analyst for the digital security firm Emsisoft.

"I think we've ended up in a vicious cycle in recent years with bigger demands leading to organizations taking on more insurance leading to them being able and willing to pay more when hit," Callow said.

Some districts, including the Judson Independent School District in San Antonio, concluded they had no alternative to paying ransom. That district's computer systems last year were encrypted by hackers and private data exported en masse. The district of 23,000 students paid $547,000.

Hackers this year have attacked at least 27 U.S. school districts and 28 colleges, Callow said. At least 36 of those organizations had data stolen and released online, and at least two districts and one college paid the attackers, Callow said.

Resources can limit what a district does to prevent and respond to an attack, said Superintendent Stephen Nellman of Centinela Valley Union High School District, which was targeted last year.

"When a school district is hit with an attack, there is no statewide support office that coordinates a response," Nellman said. "Each district is expected to coordinate their own response, and not all districts have the expertise or funding to react in a timely manner."

Centinela Valley said insurance coverage has paid off because the insurer requires the district to maintain a high level of network security, which is annually audited.

School districts are frequently reluctant to acknowledge or reveal details about an attack, including whether they paid a ransom.

Rialto Unified declined to answer questions about a recent attack because of the "sensitivity" of the issue.

"In our district, we created a recovery plan and we followed the guidance of the cyber forensic team," said district spokesperson Syeda Jafri. "We are continuing with security updates and processes."