Written by **Joe Wolverton, II, J.D.** on March 4, 2023

# Hackers Steal Public-school Student Data and Use Ransomware to Terrorize Families

If you send your children to public, charter, or private school, please read this chilling report from Bloomberg:

bymuratdeniz/iStock/Getty Images Plus

> Families of students in Los Angeles are learning this week that their kids' medical records are appearing on the dark web thanks to a notorious ransomware crew that's extorting academic institutions.
>
> Kids' medical and mental health records, in addition to 2,000 student assessments, driver's license numbers and Social Security numbers, were published after a breach last year at the Los Angeles Unified School District, said Jack Kelanic, senior IT infrastructure administrator. The district is the second-largest in the nation, with more than 600,000 pupils in 1,000 schools.

With stories like this, it is baffling why parents would persist in placing their kids in the "care" of public, private, and charter school systems.

Here's more of the story, as reported by the *Los Angeles Times*:

> "Some of these records go back almost three decades which creates further time-consuming analysis," the statement said. "Our review has also revealed positive COVID-19 test results were part of the breach. Further analysis is ongoing."
>
> It's hard to uncover the trail of effects from such data breaches, Brett Callow, threat analyst for the cybersecurity company Emsisoft, told The Times.
>
> "What impact does knowing that extremely sensitive information have on people, including in terms of their mental health?" Callow said. "How often is the stolen information misused? How often do third parties scrape the data and share it on other websites or on social media? How often [are] people actually contacted in extortion attempts?
>
> "Unfortunately, it's not unusual for attacks to result in sensitive information leaking online," he continued. "Ransomware is more of a problem than people sometimes realize, and we really do need to find better ways to counter it."

The potential for psychological damage and blackmail from hackers with access to the data and from

users of the dark web who can purchase the private data of these children is incalculable. It is not hyperbolic to fear the spreading of critical health information of your children among the vilest segments of our society.

While this breach was limited to data, it is not beyond probability that the surveillance-video recordings will soon be the target of technological terrorists.

In a 2018 *TNA* article, I predicted the possibility that video surveillance in schools could be compromised, as well:

> A manufacturer of facial-recognition technology has released a guide to help school administrators get the most out of the cameras installed in K-12 classrooms.
>
> RealNetworks provides its facial-recognition technology to schools free of charge in order to help make the country's schools safer. The guide's release was timed so as to reach school districts during The National School Safety Center's annual Safe Schools Week, observed this year October 21-27.
>
> The handbook has six policy sections: notice, consent, security, retention, transparency, and management. It includes information intended to assuage any potential concerns about privacy, and assures administrators, parents, and teachers that the purported security benefits delivered by the cameras and the facial recognition software they use far outweigh any second thoughts about the children's rights.

The installation of surveillance equipment in classrooms began to spread rapidly during the so-called pandemic.

A record number of families chose to homeschool, since schools were closed after the government's coronavirus crackdown, but the conversion of students into surveillance-technology test subjects should have made that number much higher.

In light of the Los Angeles school district students' personal and private data having been hacked and distributed on the dark web, perhaps more families will stop surrendering their children to the care of strangers for eight hours a day, five days a week, for 13 years.

The particular group who acquired access to the district's video surveillance data is appropriately called Vice Society. Here's a little information on this criminal gang and their tactics:

> Little is known about the group, which has hit at least 136 other school systems, local governments and other targets since it appeared in 2021, according to Palo Alto Networks.
>
> It's evolved into one of the most pernicious gangs in recent years, and cybersecurity experts are warning it's likely to continue to become an even nastier threat.
>
> Members seem to particularly relish bullying schools, emergency services and local governments, with the US warning in September that groups like Vice Society could disrupt school openings by leveraging known software flaws for their own gain. While most ransomware attacks subside within a few days or weeks, the group is publishing sensitive details about students — months after their school was breached.
>
> The gang's website also seeks to embarrass victims by including pictures accompanied by

> taunting messages. In other hacks, Vice Society has published passport images belonging to teachers and students. It's not clear if the group has posted pictures from the Los Angeles district breach.

None of this data should be in the control of educrats, teachers, and staff with no accountability to the parents whose children they purport to protect.

And when it comes to the spread of video surveillance, putting such systems in schools seems to have one purpose: Make students accustomed to being under constant surveillance while they are young, so that when they are adults, being watched will be something so common they won't realize that their rights have been taken from them, and thus won't think of protesting against any other surveillance program.

In light of the fact that legally these teachers and administrators stand *in loco parentis*, they should now be held accountable for their failure to protect these children from criminals who have now stolen and sold data and images of these innocent boys and girls to those who plan to do them and their families irreparable harm.