EducationWeek.

PRIVACY & SECURITY

A Massive Data Leak Exposed School Lockdown Plans. What Districts Need to Know

By Arianna Prothero — January 24, 2024 5 min read

— Nicolas Herrbach/iStock/Getty

More than 4 million school records held by school safety software company Raptor Technologies were left inadvertently exposed online. The cybersecurity leak—which the company says is now patched—included thousands of documents detailing emergency plans at U.S. schools, including lockdown procedures.

The data leak is the latest in a series of high-profile cybersecurity incidents with K-12 vendors from the past few years, including a 2022 cyberattack on Illuminate Education, and a 2018 data breach of Pearson Education.

But incidents like this raise the question: what can districts do when a vendor they trust to hold sensitive data fails to safeguard that information? It's not a question reserved just for the districts affected by the Raptor Technologies data security leak, said Doug Levin, the director of K12 Security Information Exchange, which tracks cybersecurity problems in schools.

"In general, security experts would encourage school systems to outsource these services to technology companies that may be more expert at protecting IT systems than school districts, because it is their full-time job and may have more expertise," he said. "However, it does mean that if they happen to be compromised, the scope of those incidents can be orders of magnitude larger."

In a statement to Education Week, Raptor Technologies Chief Marketing Officer David Rogers said the company is taking extra precautions in addressing the leak. "We take this matter incredibly seriously and will remain vigilant, including by monitoring the web for any evidence that any data that has been in our possession is being misused," he said.

While there's only so much schools can do to protect data that has been shared with vendors, say experts, there are steps schools should take to do their due diligence and be savvy customers.

Students' medical records, school safety evacuation plans, names of students who might pose threats were compromised

In December, a security researcher working for a company called vpnMentor reported the data leak to Raptor Technologies, which is used by more than 5,300 U.S. school districts, according to the company's website. That represents more than a third of all school districts in the country. Earlier this month, the security incident was reported by technology magazine WIRED, which found a host of sensitive information was left exposed, including:

- Evacuation plans with maps showing escape routes and meeting places;
- Information on students who had been flagged as posing a threat on campus;
- Court documents outlining family abuse and restraining orders;
- Medical records, including students' health conditions;
- The names and ID numbers of staff, parents, guardians, and students;
- And, in some cases, details such as whether a door was locked or a security camera was broken.

“The sensitivity of these data are definitely a concern,” said Levin. “This is not a case where simply offering free credit monitoring is necessarily the right remedy, even though that is the standard for companies that experience an incident.”

Raptor Technologies provides a suite of software services to school districts, including products that screen and track school visitors, monitor student attendance, and conduct behavioral threat and suicide risk assessments.

The District of Columbia Public Schools was among the districts affected—although only to a relatively small degree, the district said in a notice to families. The district had only recently started using Raptor Technologies’ visitor management software in some of its schools, so student names and ID numbers were temporarily accessible. The district has suspended the use of the software.

“Our investigation into the nature of the issue remains ongoing,” Rogers said in the statement from Raptor Technologies. “However, at this time, Raptor is supporting its customers, if needed, in reviewing the contents of the data and ensuring that any individuals whose personal information could have been affected are appropriately notified.”

Raptor Technologies also emphasized in its statement that its security protocols are “rigorously tested” by third-party reviewers.

What schools can—and can’t—do to protect themselves

It’s a dilemma for schools. On the one hand, schools need these vendors. Having the infrastructure and expertise to collect, manage, and protect student data is becoming increasingly out of reach for districts as both technology and cybercriminals become more sophisticated.

On the other hand, once that data leaves a school system’s orbit, there’s little it can do to safeguard it.

Where districts have the most power to protect school data is before they sign on the dotted line of a contract, said Amy McLaughlin, the cybersecurity initiative project director for the Consortium for School Networking, a professional association for K-12 education technology leaders. Districts should carefully read vendor contracts and conduct a risk assessment of the vendor, she said. CoSN offers a free K-12 vendor risk assessment tool.

It’s also important to have realistic expectations.

“You’re not going to have a risk-free environment,” McLaughlin said. “Just because somebody has had a security incident doesn’t mean that you shouldn’t use them. You want to know how they responded to it.”

A best practice is for a vendor to quickly acknowledge that it has identified a problem, said McLaughlin, and disclose how long it took them to lock down the system. Vendors should also commit to continuing to monitor the problem and detail what they learned from the incident and what additional steps they have put in place to ensure it doesn’t happen again.

Levin further emphasizes that efforts to improve cybersecurity in K-12 education should focus on the vendors as much as the school districts they contract with. Too often, he said, the focus has been on districts when there’s a limited amount they can do.

“What do we need to do around procurement so we can better assess an IT vendor’s security claims?” he said. “If we’re introducing risks by using these products, what is the good housekeeping seal that districts can look to, to know that vendors are taking this seriously?”

There is the Student Data Privacy Pledge that vendors can sign, but it is a voluntary commitment, not a binding one.

Regulators are also key. Several federal agencies have been focusing more on the cybersecurity practices of online companies, including those that serve K-12 education, said Levin.

“Data and information about school systems is only as secure as the weakest link,” he said.

Arianna Prothero

Assistant Editor, Education Week

Arianna Prothero covers technology, student well-being, and the intersection of the two for Education Week.

Reprints, Photocopies and Licensing of Content