Cyberattacks: A Growing Threat to K-12 Digital Learning: How Should Schools Respond?

By Mark Lieberman

Cyberattacks on school districts are on the rise during COVID-19 as students and teachers have expanded their use of technology. Federal agencies are warning schools to be on alert. The Baltimore County district in Maryland offers a case study for how to respond to a cyberattack, and what to expect if one occurs. The attack, which hit the all-remote district on Nov. 24 around 8 p.m., has cost the district at least $1.7 million, not counting millions more covered by insurance. Cyberattacks have wide-ranging impacts you might not expect if your school has never experienced one. Use this timeline to help you prepare your district’s long-term response to a costly cyberattack.

Assessing the Damage

Instruction was set to resume the following day, one week after the incident. Students and staff with Windows devices were asked to complete an online “confidence check” to determine whether the devices were safe to use. Anyone who needed help with the confidence check could report to a school building.

Coordinating District Priorities

During frequent discussions with other district departments, the IT team determined that restarting the network for scheduled SAT exams that weekend was a top priority. “Even with all of the information, it might do, the thing that might happen may not fit any of the drills you run,” Corns said.

Bringing Students Back

The district announced that no data was stolen during the cyberattack. “That was a good thing to be able to say,” Corns said. Student attendance began to inch toward pre-attack levels, reflecting that more students were gaining confidence their devices were safe to use.

Weather Disrupts Recovery

Reconfiguring student devices isn’t simply a matter of technical know-how. Weather also plays a role. A snowstorm blew through the area, forcing the district to cancel repair and replacement efforts for students’ devices until the following week.

Tackling the Ripple Effects

The ransomware attack hit squarely in the middle of benefits enrollment season. On this day, the benefits office lacked access to any elections staff had made between Oct. 12 and Nov. 15. The district announced to families its most blunt language yet: “We are not sure how long it will impact all systems, and our long-term solutions will take some time.”

Administrative Troubles

The ransomware attack hit squarely in the middle of benefits enrollment season. On this day, the benefits office lacked access to any elections staff had made between Oct. 12 and Nov. 15.

Resetting a Positive Tone

After a grueling few days, district leadership shared a note of reassurance and praise for the community. “The resilience of our students, teachers, and school-based staff is clear.”

Compromised Grading System

The district’s report card and transcript systems were finally back in order, and the district had begun “deploying state-of-the-art endpoint detection monitoring to protect against these types of threats in the future.”

More Work to Do

Third-party experts confirmed what the district had already determined. No data was stolen during the cyberattack. Report card and transcript systems were finally back in order, and the district had begun “deploying state-of-the-art endpoint detection monitoring to protect against these types of threats in the future.”

But more than two months from the last timeline entry, the work is far from over. Efforts to repair every student’s device are still underway, and the district is still working with federal investigators to get to the bottom of the hack itself.

The cyberattack has been tough on everyone in the district, and the IT team is no exception. Corns has encouraged staffers to open up to each other and intentionally take breaks on weekends to avoid getting burned out or losing hope.