# 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.

## 2020

### NOV.

**Saturday Nov. 28**

**Classes Canceled**

Midway through the Thanksgiving weekend, the district announced instruction would be canceled the following Monday and Tuesday. A decision like this is similar to reacting to a snowstorm, Jim Corns, the district's IT director said: "You're basing it on predictions, forecasts, what you're seeing in the weather at the moment."

**Sunday Nov. 29**

**An Email Workaround**

Chromebooks and Google accounts were not affected by the hack, but computers running Windows were. Neighboring districts and agencies blocked the BCPS email domain as a precaution, leaving BCPS officials with no way to communicate externally. Corns' team set up a new account on a different Google domain to keep correspondence flowing.

**Monday Nov. 30**

**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.

### DEC.

**Tuesday Dec. 1**

**Intense Local and National Media Scrutiny**

The cyberattack in Baltimore County, one of the nation's largest school districts, was widely publicized in the news media (including by this publication). Corns said larger districts in particular should be prepared for questions from reporters and community members about the nature and scope of the attack, even as the district may not have permission from government agencies to share details.

**Wednesday Dec. 2**

**Restoring Confidence**

Some families were concerned that their personal devices had also been compromised. Corns coordinated a district-wide response, even going on TV with the county executive to reiterate that personal devices were not affected, and that a coincidental uptick in spam calls didn't reflect that the attack was still in progress.

**Thursday Dec. 3**

**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."

**Friday Dec. 4**

**Tackling the Ripple Effects**

Instruction may have resumed, but the ripple effects of the attack were far from over. The district shared with families its most blunt language yet: "It was a catastrophic attack because it impacted all systems, and our long-term solutions will take some time."

**Monday Dec. 7**

**Bringing Students Back**

The district announced to families 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.

**Tuesday Dec. 8**

**Scammers Seize the Moment**

The long-term impacts of ransomware attacks often go overlooked. Scammers capitalized on public awareness of the attack and began sending spam notes to school staffers claiming to have their personal data and demanding money. The IT team urged staff members to change their email passwords.

**Wednesday Dec. 9**

**Administrative Troubles**

The ransomware attack hit square 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.

**Friday Dec. 11**

**Network of Experts**

Staff were "digging deeply into systems and solutions" to determine more technical details about the nature of the attack. Corns and his colleagues got to know relevant associates in county and state offices during this process, and he now plans to more proactively nurture relationships with them in the future.

**Monday Dec. 14**

**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.

**Tuesday Dec. 15**

**Compromised Grading System**

The district's report card and transcript systems still weren't available, and parents and students were hungry for progress updates. The district announced that principals could share grades for the first marking period on Schoology, the district's learning management system.

**Wednesday Dec. 16**

**COVID-19 Complications**

The pandemic complicated efforts to repair students' devices on-site. Corns and colleagues were "hypervigilant" to avoid contracting COVID-19, in part because losing a staffer would have made repairs take even longer. Even so, Corns said: "It's March [2021]. We're still working on restoration. I don't need to say any more than that."

**Thursday Dec. 17**

**Systems Still Down**

Principals began sharing grades for the second marking period on Schoology, which the IT team restored earlier than some other parts of the system. Staff were advised to pick up paychecks in person the next day.

**Friday Dec. 22**

### JAN. '21

**Wednesday Jan. 6. 2021 & beyond**

**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 under way, 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.

EducationWeek®

Data Visualization: Gina Tomko/Education Week, Images: Getty