
# Cyberattacks aimed at school networks

January 8, 2021

As students, families and districts shifted from traditional learning models to remote learning, experts inside and outside of the government began predicting, and seeing, a spike in cyberattacks aimed at school networks. On Tuesday, November 24, 2020, the Baltimore County Public School System became the latest – though certainly not the only – school system to be hampered by what school officials have called a "catastrophic attack on our technology system."

Though details remain scant at this point, the attack played out like many before. One by one, district systems slowly started to fall offline. The live video stream of a school board meeting cut out, teachers noticed issues with the district's grading system, and the district's website, email applications and remote learning platform shut down. The attack was extensive enough that schools were closed for several days while the district wrapped its head around the breadth of the incident.

Based on social media postings, the encrypted files appeared to have a file extension associated with a ransomware family that first surfaced in 2018. Ransomware, for those who aren't familiar, is a category of malware that locks files or entire systems until a ransom is paid. A particularly insidious feature of the ransomware, perhaps found in the Baltimore attack, is a feature that allows attackers to disable the Windows System Restore function, making recovery all the more difficult. Fortunately, school officials "do not believe that the personal data of students or employees was stolen" in the attack. Nevertheless, as is commonplace, the county is covering the cost of credit monitoring "for all county schools students and staff."

For those who are wondering, getting out from the thumbscrews of a ransomware attack is neither easy nor cheap. In addition to the fact that payment is usually demanded in cryptocurrency and demands have risen steadily, the U.S. Treasury Department's Office of Foreign Assets Control recently cautioned that paying ransomware demands could violate federal law. In fact, "OFAC may

impose civil penalties for sanctions violations based on strict liability, meaning that a person subject to U.S. jurisdiction may be held civilly liable even if it did not know or have reason to know it was engaging in a transaction with a person that is prohibited under sanctions laws and regulations administered by OFAC."

Why school districts? Simply put, they are an attractive target. A child's data is valuable, as they often won't have much, if any, credit history, and they may not realize that their Social Security number has been compromised until they try to establish credit many years later. Additionally, schools may not have the resources to properly secure their networks or upgrade their equipment. Since most learning is being conducted remotely, those vulnerabilities only grow larger.

There is an adage in the privacy and security world, stating that it is not "if" but "when" a data loss happens. Nevertheless, now is the time to review the policies and procedures that pertain to good cyber hygiene. Policies and procedures should be tested regularly with students, families and staff. Additionally, it is critical to patch operating systems and software when updates become available. Consider cyber insurance as a way to further minimize your exposure to a data incident and to assist in managing when (not if) it occurs.

# Authors


## Jeff Knight

*Of Counsel*

Columbus
614.227.2346
jknight@bricker.com