

Viewpoints

Ransomware Series Part I: School District Cyber Attacks On the Rise



A ransomware attack involves “threat actors” using malware (i.e., malicious software) to harm school district devices, networks, or servers. It can be used to steal data, damage the district’s system, or spy on district students and/or staff. These threat actors use malware to block access to a school district’s network systems and hold regained access ransom until their financial demands are met.

While not always a centerstage concern for school districts, between the years 2016 and 2022, ransomware attacks on school districts saw a staggering 393% increase. School districts have become target rich environments for threat actors as districts house large amounts of sensitive information but often do not possess the technological infrastructure or institutional knowledge base to offensively or defensively combat these issues. Accordingly, a 2024 U.S. Department of Homeland Security threat assessment report characterized school districts as “a near constant ransomware target.”



In the absence of a federal or other standardized response procedure, school districts across the country have used their best efforts to navigate these frightening and at times fiscally paralyzing events. Some states as well as the U.S. Department of Education have stepped in to support school districts facing hardship following an attack but what can school districts do to take preventative measures? Follow this five-part series to learn more about the landscape of school district cybersecurity!

"A concerning development, for example, is dual and triple extortion ransomware attacks. That is when threat groups steal and encrypt data, forcing victims to figure out both how to access their data and how to stop it from being released on the dark web or elsewhere. Student, staff and family data released in this way poses downstream risks for identity theft, credit and tax fraud, and other nefarious activity.

It's as if someone moved into your house, locked you out, stole your possessions — and then demanded payment to turn over the keys, said Richard Bowman, chief technology officer of New Mexico's Albuquerque Public Schools.

McLaughlin adds, "They're out here stealing your data and charging you for it." Nation-state adversaries and criminal or terrorist organizations attack education entities "to fund their business model," she said."

www.k12dive.com/...

Professionals



Treesineu McDaniel

Associate

Oakland

510.550.8229

tmcdaniel@f3law.com



Namita S. Brown

Partner

Oakland

510.550.8217

nbrown@f3law.com