K–12 Cybersecurity Nightmare Tales to Avoid

Cybersecurity attacks against school districts leave destruction in their wake. Here are the stories of four districts that experienced costly cyberattacks. Please note that these real-life examples are not intended to sensationalize cyberattacks, but to help illustrate the severity of the threat and emphasize the importance of having proactive plans and resources in place to prevent and mitigate cyberattacks.

The Most Expensive School Club of All Time

Kids get bored. Many play Tetris on their phones or spend countless hours on TikTok. Others are motivated to put their hacker skills to the test to execute a cyberattack and hack into a school district's most sensitive information.

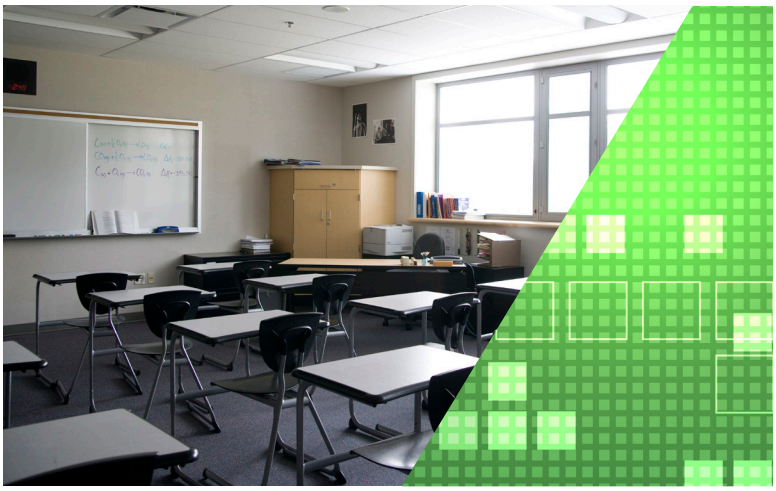
This exact event happened to one large district. District leaders were notified via email that the hackers—strongly believed to be students—claimed to have downloaded students' grades and Social Security numbers as well as the confidential information of employees, students, and parents going back almost 20 years. The hackers even provided the links to the information to prove their good work.

The estimated cost to clean up this invasive attack—$30,000,000.

Operation Chaos

The old pen and paper method of taking attendance perhaps wasn't the most efficient, but it was relatively secure.

Now, like much of our lives, these tasks are handled digitally and stored on a server. This is where one school found itself in an operational nightmare as a cyberattack compromised the student information system used to take attendance, contact families in emergencies, and make certain that students are picked up from school by authorized adults. The resulting closure of school left students without instruction and much-needed meals.



Next Stop for District Data…the Dark Web

The "dark web." Just the name itself is scary. The dark web is made up of hidden sites that are unreachable by standard web browsers. Websites on the dark web use encryption software so that visitors and owners can remain anonymous. This makes it highly conducive for illegal activity—like the selling of stolen identities and Social Security numbers.

Recently, one district suffered a devastatingly effective ransomware attack. The stolen information ran the gamut, including documentation of disciplinary actions, student gradebooks, general staff information and financial records, Social Security numbers, driver licenses, passports, student grades and home addresses—and all were posted to the dark web.

Ransomware That Obliterated a Budget

School budgets are precious. Every dollar is needed. But in the era of cyberattacks, hacks, and ransomware villains, just one successful cyber event can render budgetary planning moot.

One district recently lived this cybersecurity worst-case scenario. Ransomware hackers threatened to publish "sensitive, identifiable information" on the dark web, shutting down the district's information technology systems for a month, leaving the district without phones, emails, or Wi-Fi. The price to get the attackers assurance the data would be kept private and safe was settled at $500,000.

Strengthen Your Cybersecurity Posture

Cyberattacks can have expensive repercussions, making cyber insurance critical. It's also becoming significantly more expensive and difficult to procure. Districts are not only tasked with much higher prerequisites to be insured, but they are also facing much steeper deductibles and costs for policies. Strengthening your cybersecurity posture not only reduces the likelihood of an attack and improves your ability to recover from one—it should also reduce the cost of a successful attack and enable the district to get the best possible insurance policy available.

Many resources are available to help K-12 school districts define and evaluate their cybersecurity posture, including the K12 Security Information Exchange (K12 SIX), which offers cybersecurity resilience to keep students learning and school districts operating. You may also refer to the Cybersecurity and Infrastructure Security Agency (CISA), which—in collaboration with the FBI—has produced a helpful fact sheet: Cyber Threats to K-12 Remote Learning Education. The Consortium for School Networks (CoSN), a membership organization supporting K-12 education technology leaders, has cybersecurity reports and resources available, and districts can also seek out chapters of InfraGard to strengthen connections and expertise by building a community with cybersecurity leaders in your area.

Additionally, ENA offers a robust suite of cybersecurity products and services designed to strengthen a school district's defenses against attacks. Visit www.ena.com/cybersecurity to learn more about ENA's unified threat management (UTM), firewall, and DDoS mitigation solutions. ENA also partners with industry leaders Avertium and SentinelOne to provide critical cybersecurity assessment and endpoint protection services.

To request more information about ENA's cybersecurity solutions or to speak with one of ENA's cybersecurity experts, visit www.ena.com/ena-solutions-security-strategy or email solutions@ena.com.

ENA delivers transformative connectivity, communication, cloud, cybersecurity, and technology services supported by exceptional customer care. For more information, please visit **www.ena.com**, call **866-615-1101**, or e-mail **info@ena.com**.

ena® by zayo

062227