Is Your School District Ready for the Next Round of Cyber Attacks?

Feb 17 2022

Posted By: Patrick M. Bergin

Practice Area: School Law

It isn't if, but when, the next round of cyber-attacks will happen. One common type of cyber-attack that schools face is ransomware, where a hacker takes over a school district's computer systems and holds the systems "hostage" until the district pays a ransom or can restore the system on its own. Restoration for some districts can be nearly impossible.

Like any other multi-million-dollar organization with sensitive data, schools are unfortunately natural targets for cyber-attacks. Per one leading anti-malware provider, in 2021 alone, 62 school districts and 26 colleges and universities were impacted by ransomware. These attacks disrupted learning at 1,043 individual schools. The recovery costs following an attack can be very significant. For example, Baltimore County Public Schools spent more than $8.1 million on recovery after an attack at the end of 2019.

And it isn't just the ransom amounts that can be frightening. Public concern over compromised data security, feelings of invasion of privacy, and negative public perception can also pose real and significant consequences for school districts. Imagine the response of a guardian or parent who receives notice that his or her student's personal information has been compromised. The inability to access necessary computer or network systems may also require schools to close and disrupt both short- and long-term operations. In 2021, on average, a school in the United States experienced seven days of downtime following a cyber-attack before resuming educational operations, and significant additional time was required to fully recover from the attack.

Why Are Schools Attractive Targets?
School districts are appealing targets for two main reasons: (1) school districts often have one of the largest budgets in the community, making them an appealing financial target; and (2) the data school districts store includes highly-sensitive student and employee personal information, including Social Security numbers, health information, and other pupil data. This information can be a gold mine to cyber criminals who are interested in identify theft or simply extorting money from a school district.

What Should School Districts Do?
School district administration should embrace cybersecurity best practices to protect their schools from cyber-attacks. This requires administrators to review current practices and thereafter remain vigilant in conducting an ongoing review of such practices. Here are a few things school districts can do to help protect themselves:

- **Develop a communication plan.** Time is critical when a cyber-attack occurs. It is essential that you are ready to address guardians and parents, the media, and the community, and to work with your insurers and law enforcement immediately when an attack happens. Different laws require notice to individuals affected by privacy breaches. Your district should pre-emptively develop a communication plan so it is immediately ready to address required stakeholders. This communication plan should be routinely discussed with relevant administrators and employees.
- **Update Systems.** Network users should apply software patches and updates as soon as possible. Hackers often exploit systems that don't timely install patches and updates.
- **Create a strong password policy.** Password policies must require users to update in regular intervals and integrate best practices, including passphrases, sequences and having different passwords for multiple accounts.
- **Purge outdated technology.** Schools may hang on to older devices due to budget constraints. However, older devices may not be as secure as newer systems.
- **Implement multi-factor authentication to protect network access.**

Some tips to help districts recover more quickly include:

- **Back up essential data frequently.** The ability to restore data is a significant factor in determining whether a school district should pay a ransom.
- **Train employees.** Train staff to recognize phishing emails and other types of cyber-attacks.
- **Develop a cyber-attack response plan.** Schools should work with their IT staff, IT providers and legal counsel to pre-emptively develop a plan to handle varying cyber-attacks and return to normal operations.
- **Evaluate cyber liability insurance coverage.** Based on publicly available information, ransom demands vary dramatically: as low as $10,000 to millions of dollars.
- **Stay in close contact with experienced legal counsel.** To the extent protected personal information was accessed or taken, notification to the victims and, in some states, notification to data protection authorities may be required. Legal counsel familiar with these situations help coordinate communication with law enforcement and communication with staff, students, and the public. Legal counsel also communicates with the threat actors, coordinates with your insurance company, and assists with records requests that may come in post-attack.

Most importantly, school districts should engage with their insurance agent, legal counsel and IT staff now to develop and gain a mutual understanding of the process that will be followed at the time of a cyber-attack, as well as best practices that are to currently be utilized by district employees and officials. These pre-emptive, relationship-building opportunities may expose vulnerabilities and will best prepare your district for a cyber-attack. A proactive approach may also help your district avoid an attack altogether or, at a minimum, reduce the damage.
