Cybersecurity Awareness Month – Ransomware Attack on Second Largest U.S. School District

Schools and universities are increasingly the targets of ransomware attacks. So, it is not surprising that the second largest school district in the U.S., the Los Angeles Unified School District (LA Unified) was hit by a ransomware attack that is causing ongoing technical disruption. A review of the LA Unified ransomware incident provides a detailed view of how far-reaching a data security breach can be.

Earlier this year, the FBI issued a warning to schools regarding potential ransomware threats from a group called Vice Society. Ransomware is a type of malware that encrypts data to prevent users from accessing files, operating systems or applications. Attackers then demand a ransom payment in cryptocurrency, typically subject to a time limit, for the user to regain access to their files.

Over Labor Day weekend, Vice Society targeted LA Unified in a ransomware attack. District officials detected the intrusion as it was happening and shut computer systems down. However, district officials estimated the hackers obtained about 500 megabytes of information – the amount of data stored on a single personal computer. Shortly after, the FBI and the Cybersecurity and Infrastructure Security Administration published a joint advisory warning that Vice Society had been "disproportionately targeting the education sector with ransomware attacks."

Vice Society issued a ransom demand to LA Unified two weeks after the attack, which the school district refused to pay. After reiterating that it would not cooperate by paying a ransom, Vice Society published some of LA Unified's data on the dark web. Published data included students, employees and contractors' personal identifying information, including passport details, Social Security numbers and tax information.

LA Unified continues to work with federal agencies and law enforcement in response to the ransomware incident. It created a task force to provide monthly status updates on the ransomware incident. The district will also provide mandatory cybersecurity training for employees and undergo an assessment of existing technology and current infrastructure.

The following outline provides several cybersecurity best practices to mitigate ransomware attacks disproportionately targeting schools and universities. Schools should prepare for ransomware incidents in advance and apply these practices to the greatest extent possible.

- Implement offline data backups. Backups may allow a school to access encrypted data, as opposed to paying high ransom demands to reach the same information.
- Retain multiple copies of data backups and servers in a physically separate and secure location (i.e., cloud storage, hard drive, etc.).
- Ensure third-party vendors and outside software or hardware vendors are monitored and reviewed for malware activity.

- Procure adequate first-party cyber security insurance to mitigate the costs associated with incident response efforts.
- Monitor external remote connections to investigate when an unapproved connection or application is installed.
- Provide cybersecurity awareness training to students and staff. Schools should aim to hold regular, mandatory cybersecurity awareness training sessions.
- Create and implement a cyber security incident response plan. The incident response plan should include developing legal response procedures and strategic communication procedures in the case of a ransomware attack.

The nightmare that LA Unified is currently experiencing should serve as a sobering reminder that no organization is immune to the threats and actions of cybercriminals. School districts should be regularly assessing their risk and updating their cybersecurity protocols to meet the increasing threat to sensitive student and employee records.

If you have any questions about the information presented in this memo, please contact Jessica Copeland, Maureen Milmoe or any attorney in the Cybersecurity and Data Privacy practice.

BOND SCHOENECK & KING ATTORNEYS