Discussion Time
Cybersecurity & Ransomware

Are you protected? Are you prepared?

Ransomware attacks increasing!

- **US government warns ransomware attacks on schools may increase**
- A ransomware gang known as Vice Society, which emerged last year, has been "disproportionately targeting the education sector with ransomware attacks," said the public advisory from the FBI, US Cybersecurity and Infrastructure Security Agency, and the MS-ISAC, a cyberthreat-sharing body.
- Schools with limited cybersecurity resources are often the most vulnerable to ransomware, federal officials said, but even well-defended school systems can be at risk to opportunistic hackers.
- K-12 schools "may be seen as particularly lucrative targets" because of the sensitive student data stored on school systems or through third-party tech companies, the advisory said.
- Ransomware attacks have been an added worry for school administrators already struggling to deal with the coronavirus pandemic.

What Happened to LA Unified?

- 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.

- The Government Accountability Office, a federal auditor, has called on the Department of Education to do more to protect schools from hacking threats.

What are we to do?

- Should School Districts Pay a Ransomware Demand? It's Not Always Simple
- Ransomware Attack on Second Largest U.S. School District

What are we to do???

- 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.

Best Practices to Prepare for Ransomware

- 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.

How the Cloud Can Stop Ransomware

- Relying on cloud services, or using Chromebooks that are essentially machines that only run a browser, are ways schools can avoid severe damage when hackers hit. Another is to have backups that are on a separate network, meaning they don't get hit when ransomware infects the other machines. That's what happened to Affton High School in Missouri, which didn't even have to consider paying hackers given that their backups were not impacted by the ransomware.
- (Source: https://www.vice.com/en/article/88qvmx/how-ransomware-is-causing-chaos-in-american-schools)