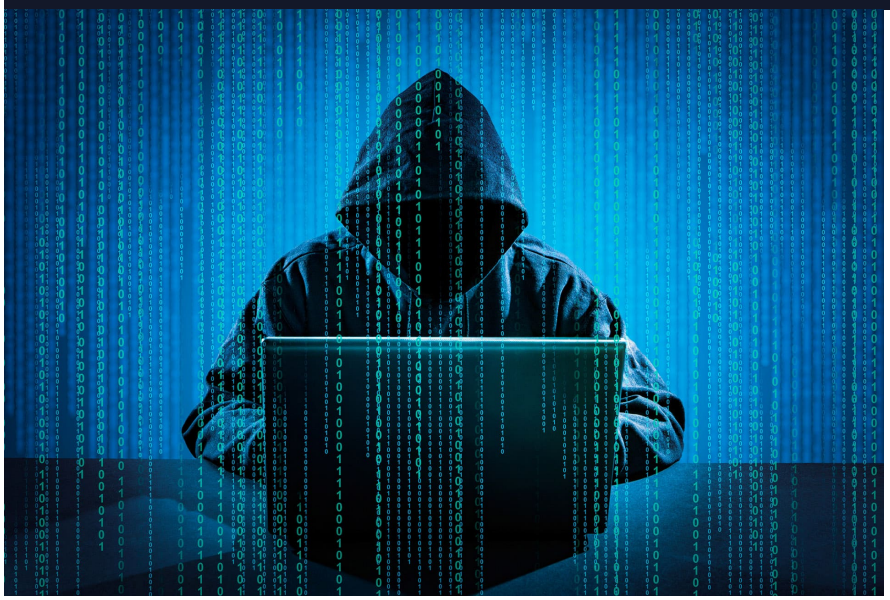
BARNES & THORNBURG LLP



ALERTS

Ransomware Attack On Nevada School District Highlights Newest Hacker Targets

October 2, 2020

Highlights

A Las Vegas, Nevada, school district, serving over 320,000 students, has become the victim of the largest ransomware attack against an educational institution since the COVID-19 pandemic began

The pandemic has opened new opportunities for cybercriminals and attacks are expected to continue to increase in frequency and severity

Strong proactive steps should be considered, which can provide an advanced and effective defense

On Sept. 28, 2020, personal student information – including grades, Social Security numbers, and other private information – from the Clark County School District in Las Vegas, Nevada, the nation's fifth largest public school district, was released online by hackers. The school district serves over 320,000 students.

The information had previously been hacked and stolen, and when the school district refused to pay a ransom, the hackers published the information.

RELATED PEOPLE

Jason A. Bernstein
Partner
Atlanta

P 404-264-4040
F 404-264-4033
jason.bernstein@btlaw.com

Todd G. Vare
Partner
Indianapolis, Chicago

P 317-231-7735
F 317-231-7433
todd.vare@btlaw.com

Brian J. McGinnis
Partner
Indianapolis

P 317-231-6437
F 317-231-7433
brian.mcginnis@btlaw.com

RELATED PRACTICE AREAS

Data Security and Privacy

Recently, ransomers have been using the threat of publishing the files as an incentive to extract the demanded ransom. The amount of ransom demanded has been increasing markedly over the past year as hackers have been emboldened by their success.

According to a Sept. 28 Wall Street Journal article, Clark County is the largest school district to be hit with ransomware since the pandemic began, however, it is not the first. Since 2016, cyberattacks on school districts have been steadily rising in frequency and severity. According to the K-12 Cybersecurity Resource Center, as of fall 2020, over 1,000 cybersecurity incidents have occurred since 2016, and that number is expected to continue to climb.

According to a notice posted on the Clark County School District's website, its computer systems were infected on Aug. 27 with ransomware, locking up the infected files and rendering them inaccessible unless money was paid to the ransomer.

With the majority of school districts across the country adapting to some form of distance education, there is an even greater strain on schools' already limited technical resources, making them more vulnerable than ever. Recognizing this vulnerability, the FBI issued a warning to all K-12 schools regarding the expected increase in ransomware attacks during the coming months, saying that "cyber actors are likely to increase targeting of K-12 schools during the COVID-19 pandemic," and urging school districts to take extra precautions to secure their networks.

The potentially devastating effects of a ransomware attack make it clear that the best defense is a strong offense. Since ransomware infections are often the result of personnel inadvertently opening an attachment or a link in an email that deploys the ransomware, organizations should consider taking the following actions to help prevent and prepare for such an incident:

1. **Increase Frequency of Data Backups:** A critical component to averting disaster in the event of a ransomware attack is to back up essential data offsite or offline frequently, particularly of data that changes daily. Being able to quickly restore the majority of locked up data is the most important factor in determining whether to pay a ransom.

2. **Increase Employee Training:** Train personnel more frequently on recognizing bad emails. As noted, the most frequent cause of successful cyberattacks is untrained personnel inadvertently clicking on a bad link or infected file in an email.

3. **Incident Response Plan:** If your school or organization does not already have an incident response plan, one should be put in place as soon as possible. It is a best practice to include procedures on who, how and when personnel should report an incident, and what should be done in response. It is also a best practice to have someone heading the response team who is experienced in responding to breaches, especially ransomware attacks.

4. **Implement Multi-Factor Authentication**: Implement multi-factor authentication (MFA) processes to help protect account access.

5. **Password Strengthening:** Require strong passwords with regular change intervals. Do not use the same password for multiple accounts or common names or sequences in passwords. A suggested best practice would be to use a passphrase, which is longer and more difficult to break.

6. **Vulnerability Patching:** An organization should consider applying software patches and updates as soon as possible. Hackers often exploit known vulnerabilities because organizations often do not install the patch promptly.

7. **Penetration Testing:** If your school or organization has the capabilities internally or through an experienced forensics consulting firm, attempt to breach the security of your organization's systems to identify vulnerabilities. Also, ensure that regular scans of your systems are done.

8. **Insurance Coverage:** As a best practice, review insurance policies to make sure there is coverage for ransomware events and that policy limits are sufficient based on your needs.

For more information, contact the Barnes & Thornburg attorney with whom you work or Jason Bernstein at jason.bernstein@btlaw.com or 404-264-4040, Todd Vare at tvare@btlaw.com or 317-231-7735, Brian McGinnis at bmcginnis@btlaw.com or 317-231-6437, or Mario Arango at marango@btlaw.com or 317-229-3149.