



Viewpoints

Ransomware Series Part V: Prevention Strategies for School Districts



A ransomware attack is a breach of student information that holds “hostage” the information on payment of a ransom by the district, for school districts ransomware attacks are a common approach for cybercriminals. As there is no guarantee that hackers honor an agreement to reverse the effects of their intrusion, it is recommended by the FBI that school districts (or other victims) do not pay ransoms.

However, there is some debate about whether there are circumstances that would give rise to cooperation and payment of a ransom to cybercriminals. Here are a few prevention strategies to implement to make your district’s cyber security a bit safer:

1. Implement phishing tests—planned dissemination of suspicious emails to staff to assess their ability to identify potential threats;
2. Establish a Backup Network;



3. Explore state and federal supports (cybersecurity advisors, cybersecurity audits, and network monitoring supports); and
4. Consider the impact on the individuals whose information was stolen or accessed in your resolution strategy.

For additional details on these prevention strategies and more check out the attached link.

The FBI and other federal agencies recommend ransomware victims refuse to cater to ransom demands because payments will not guarantee that sensitive data is decrypted, systems will no longer be compromised, or data will not be leaked.

But some education finance and cybersecurity experts say the decision is not always easy. For instance, it may be less expensive and disruptive to pay a ransom to have a compromised system restored than to deal with the potential security and financial fallout of not doing so.

www.k12dive.com/...

Professionals



Treesineu McDaniel
Associate
Oakland
510.550.8229
tmcdaniel@f3law.com



Namita S. Brown
Partner
Oakland
510.550.8217
nbrown@f3law.com