Practices in Multiple States Fall Victim to Ransomware Attacks

By

Current headlines contain many stories of cyber-attacks, including data breaches and ransom malware, more commonly known as ransomware. Once your practice is hit by a cyber-attack, you'll want to be able to quickly diminish the damages inflicted on your practice and your patients. Such damages include interruption of your practice; IT forensics to assess whether PHI was compromised; and costs for recovery of records, ransom, future monitoring and/or the subsequent patient notifications. In addition, there are potential regulatory fines and penalties. An important step to protect your practice is to secure a cybersecurity insurance policy, which will guide you through the process of recovery and help mitigate the damages.

Many cyberattacks target healthcare related companies and involve millions of patient records. The records of healthcare entities of all sizes have been held hostage by ransomware - from solo practices to hospital systems, and across multiple state lines. Here are some recent examples, some from SVMIC's own policyholders:

- The server for a medical practice in Alabama was down for five days before they realized that their system had been hacked and their records were being held for a $7,000 ransom. Fortunately, their EHR vendor encrypted all of their data, and they determined there was no risk of a data breach. They are working to restore all of their data from back-up.
- Another practice in Arkansas fell victim to a ransomware attack when they clicked a link agreeing to complete updates from what appeared to be Microsoft. Once they clicked the link, their files were encrypted and ransom was requested. They are working to restore files from back-up and conducting additional investigations to ensure that PHI was not accessed.
- What started as another ordinary day at the office at one Middle Tennessee medical practice soon turned into pandemonium when an employee received a notice of ransom malware upon logging into the computer system. A cybercriminal was holding ninety-nine percent of their patient records hostage, asking for ransom in order to release them.

Fortunately, this practice had a good back-up system in place. The records were backed up nightly which allowed for recovery of up-to-date information. The practice notified the IT

firm with which they contracted, and they were able to recreate the records from back-up without paying the ransom and with minimal downtime to the practice.

- In East Tennessee, an employee of a physician's office opened an email and attachment from a presumed vendor that handled collections for the practice. However, the email was really a phishing email in disguise, and the attachment contained ransom malware. Luckily, as in the previous case, the practice had an IT vendor who was able to restore their records from back-up.

- A large practice in Arkansas received a phishing email disguised as an email from a trusted source. Once the attachment was opened, it released ransomware, which encrypted all of their patient records and prohibited the practice from accessing them. The ransom of $500 was paid to release the records.

According to Kayla Thrailkill in her article "Ransomware Attacks Increased by 167% in 2016" for Techtalk.pcpitstop.com, the number of ransomware attacks grew from 3.8 million in 2015 to 638 million in 2016. In most ransomware cases, the ransomware comes in the form of an attachment to an email. Once the attachment is opened, the ransomware encrypts or builds a firewall around the data so that the data owner cannot access it.

The HIPAA Breach Notification Rule requires HIPAA covered entities and their business associates to provide notification following a breach of unsecured protected health information. In ransomware cases, the practice must "demonstrate that there is a low probability that the protected health information (PHI) has been compromised", according to the ransomware fact sheet found on the HHS website[1]. The risk assessment, according to the fact sheet, must contain at least the following four factors: "the nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification; the unauthorized person who used the PHI or to whom the disclosure was made; whether the PHI was actually acquired or viewed; and the extent to which the risk to the PHI has been mitigated." Due to the technical nature of a ransomware attack, it may be necessary to engage the services of a digital forensic company in order to demonstrate a low probability that PHI has been compromised.

There are steps you can take to prevent becoming a victim of a ransomware attack. Employee education is important. Cybercriminals are getting smarter and are able to disguise their phishing emails to appear to come from one of your vendors or another trusted source. Caution should be used before opening any attachment, and verification of the email source should be done for all incoming emails, especially those with an attachment.

While not all practices can afford to employ their own IT security expert, it pays to have an evaluation by a qualified firm and establish a relationship. Contracting with an IT firm that is able to deal with any cybersecurity situation in a timely manner allows for minimal down time for the office. As illustrated in the cases above, regular back-up of data is key in battling a ransomware attack. In his article titled "How to prevent ransomware: What one company learned the hard way" on PCWorld.com, Robert Lemos quoted one expert at a

network-security firm who advises that online back-ups that occur automatically are best.

Even with the most prudent measures in place, you can still become a victim of a cyberattack. Although not all attacks can be prevented, a partnership with a cybersecurity insurance company can facilitate your response and mitigate the damages. Cybersecurity policies may offset the costs of recovering your data and breach notification expenses as well as some incurred fines and penalties.

SVMIC's professional liability policy includes supplemental cybersecurity coverage in the amount of $50,000. Through our partnership with NAS Insurance Services, SVMIC is pleased to be able to offer access to discounted premiums on increased limits for cyber and regulatory insurance policies to our policyholders. Please contact the Underwriting Department at SVMIC at 800.342.2239 for more information.

[1] https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf

---