Ransomware 101—Hackers Are Trying to Take Your Practice Data Hostage

Many physicians and administrators are familiar with the data lockdown that occurred at Hollywood Presbyterian Medical Center in California last year, when some of the hospital's systems were hit by hackers who demanded a bitcoin ransom in exchange for unlocking their data. Until a $17,000 ransom was paid, the facility was forced to revert to paper records to manage patient care.

Unfortunately for small and mid-sized practices, hacking is no longer limited to large institutions. "Because so many companies have already been hacked, you should go to work every day with the assumption that your data has been compromised. If you have not yet been a victim, it is only a matter of time before you are identified as a target and a cybercriminal tries to figure out how to delve deeper into your personal information," warned Jeffery Daigrepont, EFMP, CMPE, senior vice president at Coker Group, an Atlanta-based health care advisory firm.

What is ransomware? Ransomware is covertly installed malware (malicious software) that prevents you from accessing data stored on a computer system. You will be offered a decryption key to regain access if you pay a ransom.

Aim to avert attacks, but also prepare for the worst. Despite your best efforts to ward off ransomware attacks, prevention is not always possible. Even if you keep up with the latest software, you may not always be protected. Malware mutates so quickly that antivirus programmers cannot always keep up with the changes, said Janet A. Betchkal, MD, whose solo practice in Jacksonville, Florida, was hacked in 2015 (see sidebar). And once you have been hit, the likelihood for subsequent attacks increases.

Who Hacks and Why

It is not like the movies. "People often think of hackers as they are portrayed in the movies—as sophisticated code-cracking geniuses running high-end programs designed to crack top-secret government codes. In reality, cybercriminals typically engage in low-tech endeavors predicated on catching their victims off guard. They look for quick hits and generally only spend a few hours attempting a hack before they move on to another unsuspecting individual or organization," said Mr. Daigrepont.

Hackers may consider your practice to be low-hanging fruit. Hackers' success is contingent on exploiting weaknesses. "They have discovered that smaller practices and groups do not consistently have the level of investment to protect themselves like larger entities do. As a result, smaller practices may cut corners with hardware, software, and IT [information technology] support staff," said Mr. Daigrepont. For

A Glaucoma Practice Is Targeted

Dr. Betchkal knows all too well the havoc that can be wreaked after malware infiltrates a computer system.

Lightning strikes twice. "We were hacked twice in 2015 by 2 different cybercriminals—the first used Cryptowall 3.0 and the second used DMA Locker. We were forced to pay a ransom to unlock our data, and in both cases, the ransom doubled before the payment could be delivered. I had 397,000 documents stored and felt like I had no choice other than to pay the ransom to regain access to my data." This occurred even though her employees had recently performed a security risk assessment, and the practice tentatively met the relevant requirements of the EHR meaningful use program.

Pinpointing the cause. "The first attack occurred when an employee opened a job applicant's resume," she said. The cause of the second incident remains uncertain, but it is thought that a medical supply order placed with a trusted vendor via the internet was intercepted by a hacker who had tapped into their system.

BY LESLIE BURLING-PHILLIPS, CONTRIBUTING WRITER, INTERVIEWING **JANET A. BETCHKAL MD, JEFFERY DAIGREPONT, EFMP, CMPE,** AND **RAVI D. GOEL, MD.**

small companies, hackers set a relatively low ransom—usually under $5,000—which victims can, and do, pay, he said. For the hacker, those smaller amounts add up quickly as the hacker strikes multiple sources.

Reduce Your Vulnerabilities

Every practice is susceptible to a ransomware attack, but a few basic steps can minimize the risks. First and foremost, every practice should be HIPAA compliant and protect patient data to the greatest extent possible.

Perform a security risk assessment. Performing a security risk assessment is an excellent place to start when evaluating your practice's level of cybersecurity. Furthermore, if you are participating in the advancing care information (ACI) performance category of the Merit Incentive-Based Payment System, performing a security risk assessment is a required ACI measure. The ACI performance category has replaced the meaningful use program for electronic health records (EHRs).

Ravi D. Goel, MD, a comprehensive ophthalmologist at Regional Eye Associates in New Jersey, referred to 7 basic pearls for performing a security risk assessment based on the Centers for Medicare & Medicaid Services' HIPAA mandates:

- Define the scope of the analysis.
- Gather data.
- Identify potential threats.
- Assess existing security measures.
- Determine the likelihood of a threat occurrence.
- Determine the level of risk.
- Identify and document improved security measures.

However, completing this process is the minimum a practice should do to address cybersecurity.

Do not use personal email accounts. The greatest exposure to ransomware comes from physicians and staff using personal email accounts to correspond with each other within a practice, according to Mr. Daigrepont. "In particular, do not use Gmail or Yahoo email accounts for practice business. Use a corporate server with a firewall and up-to-date virus protection."

Be careful about clicking links and opening documents. Hackers frequently use social engineering techniques such as phishing to trick people into clicking on a seemingly harmless link—and this, in turn, launches a cyberattack. Dr. Goel gave the following example. "In my practice, we look for new technicians by posting ads on Craigslist. I used to open those without hesitation until I found out that a practice was hit by ransomware because a 'potential employee' emailed a CV [curriculum vitae] via Craigslist. All incoming documents should be scanned with antivirus software and treated as a potential threat."

Additional safeguards to consider. Dr. Betchkal, Mr. Daigrepont, and Dr. Goel shared the following tips.

- Use different passwords for each device, and change passwords often.
- Create multiple backups and test them regularly to ensure that you can easily restore your system.
- Store a backup of your system offsite.
- Consider cloud storage from a vendor that meets industry standards and offers comprehensive security protections that can be verified.
- Purchase insurance that covers cybersecurity breaches, and take advantage of any staff training offered.
- Utilize monitoring tools that scan your network in real time to detect intrusions.
- Enlist the assistance of a consultant.
- Employ an IT expert to protect your practice. This person should be reachable 24/7 to quickly address problems.
- Discuss cybersecurity with your EHR vendor, ask about the vendor's role in your protection, and implement additional precautions where necessary.

Key Terms

Bitcoin—digital currency that appeals to extortionists because it enables them to maintain anonymity when receiving payment

Cybersecurity—the protection of computer hardware, software, and data from intentional or accidental theft or damage

Dark web—similar to the world wide web but requires special codes, configurations, or authorization to enter and is used for criminal activities, including fraud, illegal pornography, and drug sales

Malware—software created for the purpose of disrupting computer operability for malicious purposes

Phishing—technique used by cybercriminals to obtain sensitive information by impersonating a trustworthy source in an electronic communication

Social engineering—a type of fraud based on the manipulation of individuals in order to coerce them into revealing personal or confidential information

How to Respond

In the case of ransomware, you will likely know instantly if you were hacked because the goal of a hacker is to quickly secure a ransom payment.

Step 1: Shut everything down. "If you are hit by a ransomware attack, the first thing you should do is shut everything down and immediately ask your IT employee or contractor to perform a full assessment," said Dr. Goel.

Step 2: Buy bitcoins. "The minute you find out you have been hacked, look into buying bitcoins," said Dr. Betchkal. "Even if you find that you do not have to pay the hacker to unlock your data, put them in an account because obtaining them is difficult."

Dr. Betchkal is in private practice in Jacksonville, Fla. *Relevant financial disclosures: None.*

Mr. Daigrepont is senior vice president at the Coker Group, a nationwide consultancy group based in Atlanta. *Relevant financial disclosures: Coker Group: E.*

Dr. Goel is in private practice in Cherry Hill, N.J. *Relevant financial disclosures: None.*

See the disclosure key, page 10.

EXTRA **MORE ONLINE.** To pay or not to pay? That is the question discussed in this article's Web Extra at aao.org/eyenet.