Cyberattack! Be Prepared for Attempted Hacks

A practice's electronic data contain a treasure trove of valuable assets—health data, credit card and bank account numbers, street and email addresses, driver's license documentation, Social Security numbers, and even information on family members. Therefore, it's no wonder that the health care industry is the most targeted sector for data breaches.[1]

A deadly problem. A study at Vanderbilt University estimates that breaches at U.S. hospitals may cause as many as 2,100 patient deaths each year.[2]

An underacknowledged problem. Physicians handle protected health information [PHI] on a daily basis, and they are legally required to keep that data safe, said Renee Bovelle, MD, at Howard University Hospital Department of Ophthalmology in Washington, D.C. "Yet, despite the serious ramifications for your reputation and your career, cybersecurity isn't part of our formal training, and too many of us shrug off the consequences until it's too late."

What Makes You Vulnerable

Your biggest vulnerability? You and your staff. The biggest cyber vulnerability for any practice is people, plain and simple, said Marissa Maldonado, senior vice president of the Coker Group, an Atlanta-based health care advisory firm. "The human behind the keyboard is the one who will ultimately open the doors," she said. "And hackers will exploit your staff first and foremost with a phishing attack."

Phishing can trick you into sharing sensitive data. Phishing involves the use of email or unsafe websites to collect personal and financial information or promulgate malicious software, known as malware, said Jeffery Daigrepont, EFMP, CMPE, senior vice president at Coker Group.

Phishing can be personalized. "Think of phishing as a type of social engineering in which the hacker, masquerading as a trusted entity, studies an individual and personalizes the attack," said Mr. Daigrepont. For example, an attacker might notice that one of your employees posted on social media about a family member who was recently diagnosed with cancer. They'll then customize a flyer for a cancer charity benefit and send the event to your staff member's work email with the intention of digging up any confidential information they can use to breach your practice. "Unfortunately, even the smartest of people get fooled with these phishing scams," said Mr. Daigrepont. "The attackers are searching for low-hanging fruit. They're playing on your emotions. And unfortunately, there's not a single piece of technology that can prevent a person from making a bad decision."

What's in it for the hacker? Money of course! "During a phishing attempt on your practice, hackers are casting out their fish nets, seeing who will respond to the exploit—clicking on a link, responding to an email, opening a document," said Ms. Maldonado. "After a bite, they'll then evaluate the value of the catch. Is it a little minnow or a trophy?" And ransomware has become a game changer in the hacker world because it's a very efficient way to monetize a data breach.

What is ransomware? If you fall prey to a phishing ruse, you may inadvertently upload ransomware to your computer system. Ransomware is a type of malware that can prevent you from accessing your data unless you pay a ransom for a decryption key. "It's a great business model in the eyes of the hacker," said Mr. Daigrepont. "They supply you with detailed, easy-to-follow instructions and the digital payments aren't traceable."

To pay or not to pay? If hackers consider you a "big fish," they might hold your servers, your EHRs, and your workstations hostage via malware and then demand a ransom to unlock the encryption. Mr. Daigrepont estimates that about 50% of practices choose to pay the ransom and retrieve their data because, in the end, it's cheaper than having an IT expert find a fix. But even then, the hackers might double dip. "You might get your data back and reopen your practice, but there's no guarantee that the hackers won't re-monetize your records by selling them on the dark web," he said.

Don't assume cloud storage is immune to attack. Those practices that

BY MIKE MOTT, CONTRIBUTING WRITER, INTERVIEWING **RENEE BOVELLE, MD, JEFFERY DAIGREPONT, EFMP, CMPE,** AND **MARISSA MALDONADO.**

refuse to pay a ransom for their data often think they can rely on their cloud storage to restore stolen data, but those backups are becoming increasingly compromised as well during an attack. For example, hackers might obtain the security token that is used to access your cloud storage or, if you are syncing your files to a cloud-based platform, they might first infect your local files.

How to Prepare

In the cybersecurity world, it's not a matter of if an attack will occur but when, said Dr. Bovelle. "We are all susceptible, so an ounce of prevention is worth a pound of cure."

Hire a professional. First things first, speak with a real expert to assess the overall state of your practice's current cybersecurity, said Dr. Bovelle,

What your response plans should cover. Ms. Maldonado said that a professional can help you put together your disaster recovery and incident response plans. These are living documents that outline:

- who is on your incident response team;
- how to analyze and validate an incident to make sure you're triggering the correct response;
- how to contain the incident, eradicate the threat, and recover from the attack; and
- how to assess the severity and damage and begin the notification process.

Keep on top of your security risk assessment. In addition, the consultant can help fine-tune your security risk assessment (SRA), said Dr. Bovelle. This assessment is an evaluation of where your practice's PHI could be at risk, and providers are required to perform an SRA if they are considered a "covered entity" under the Health Insurance Portability and Accountability Act (HIPAA). Furthermore, under the Merit-Based Incentive Payment System (MIPS), you must conduct or review an SRA in order to score more than 0% for promoting interoperability, which is MIPS' EHR-based performance category.

What your SRA should cover. The Office of the National Coordinator for Health Information Technology (ONC) offers a helpful online tool to guide you through the process, said Dr. Bovelle.[3] All SRAs should share the following:

- Scope of the analysis, including all of the electronic PHI that your practice creates, receives, maintains, and transmits
- Documentation of potential threats and vulnerabilities
- Assessment of current security measures
- Determination of the potential impact of a threat occurrence and the level of risk
- Periodic review and updates to the SRA

Plug any gaps. When your SRA is complete, it's paramount that you follow through and correct anything you discover, said Mr. Daigrepont. "If you document that a vulnerability exists and choose to ignore it, when an attack occurs, you're basically acknowledging you had a weakness and did absolutely nothing about it," he said. "There's virtually no forgiveness from an auditor when that happens. They will be very harsh."

Don't assume that vendors have your back. Never assume your vendors are taking care of your cybersecurity for you, said Mr. Daigrepont. "You might think that, because you have a cloud vendor or a vendor hosting your IT system, they are taking care of everything related to privacy and security," he said.

Key Elements of Cyber Liability Insurance

In addition to potential safety issues, a breach can result in a substantial increase to your operating costs due to response and recovery activities, service disruption, reputation damage, and potential regulatory fines and patient claims. Cyber liability insurance can help you cover a portion of these losses and is an essential part of any cybersecurity program.

What your insurance covers. Many medical malpractice insurers will include cyber liability coverage up to a certain limit, and they may offer you the option of offering additional coverage. The Ophthalmic Mutual Insurance Company, for example, contracts with Tokio Marine to provide additional coverage (www.omic.com/partners/cyber-liability-update/).

What coverage you should consider. Mr. Daigrepont said that the key elements that health care providers should consider when shopping for a policy include the following:[1]

- **Business interruption:** coverage for costs, such as an inability to provide services for a period of time due to a ransomware attack.
- **Contingent business interruption:** coverage for lost revenue if a vendor that you heavily rely on experiences a breach that causes your organization to suffer financial loss.
- **Cyber extortion:** coverage for the cost of ransomware, which includes hiring a negotiator, and even the ransomware payment.
- **Incident response:** coverage for costs incurred for response and recovery from a data breach, including forensics, incident containment and remediation, victim notification, public relations, and credit monitoring.
- **Legal expenses:** coverage for costs defending against a lawsuit brought by your customers as a result of a data breach.
- **Regulatory fines and penalties:** coverage for fines if it's determined that the practice failed to adequately protect patient data during a breach by not fully adhering to baseline cybersecurity laws and requirements.
- **Liability and expense cost:** coverage for losses and cost of defense for lawsuits related to network security liability.
- **Cybercrime:** protection for types of cyber events that include financial fraud such as electronic theft, fund transfer, and invoice manipulation.

1 https://cokergroup.com/key-elements-of-a-cyber-liability-insurance-policy-for-health care-providers/. Accessed Nov. 10, 2022.

"That's a major mistake." For example, your EHR vendor might provide assistance and training on the privacy and security aspects of your EHR product, but they are not responsible for making sure the use of the product is HIPAA compliant.

Who handles your PHI? "Not only do you have to worry about yourself, but also you have to worry about all of these third parties handling your data," said Dr. Bovelle. For example, one of the largest health care breaches to date occurred in 2019 when hackers gained access to more than 25 million health records from American Medical Collection Agency—the debt collector for LabCorp, Quest Diagnostics, and other medical service providers.[4] "This is a sad example of what can happen when your business associate does not adequately protect your PHI," said Dr. Bovelle. "Not only did the agency declare bankruptcy, but also each of the [HIPAA-]covered entities was under investigation by the Department of Health and Human Services."

Solidify your business associate relationships. It is important that your practice establishes security compliance with all of its business associates—including billing companies, collection agencies, and EHR vendors, to name a few—and has them sign your business associate agreement (BAA), said Dr. Bovelle. This forms the legal contract between your practice and any other organization that receives access to transmit or store your PHI. You'll also want to ask for a copy of the associate's own risk management plans and ask whether or not they conform to third-party auditing certification, like the gold-standard HITRUST (Health Information Trust Alliance) certification.

Additional protections. There are many other security safeguards to consider as well, said Ms. Maldonado.

Get rid of free email. Because email is one of the most common entry points for attackers, replace free email platforms—like Gmail, Yahoo, Hotmail, and AOL—with professional servers that employ proper security safeguards and spam filtering.

Bolster your insurance. Adding cybersecurity coverage to your policy can help protect you against significant financial loss resulting from an attack. (See "Key Elements of Cyber Liability Insurance" for more information on selecting the right insurance coverage.)

Purchase insider threat monitoring. There are many inexpensive threat detection platforms on the market that can alert you to suspicious activity and anomalies occurring on your workstations.

Enforce two-factor authentication (2FA). 2FA adds a layer to your security by requiring a security token, such as a one-time code that is sent to you by email or text, or a biometric scan to verify access to devices and applications.

Reassess your culture. Most data breaches result from honest mistakes made by your employees. So consider a "no questions asked" policy that allows your staff to feel safe and comfortable when reporting their mistakes. Punitive discipline more often than not will result in breaches that go ignored.

Make training fun. Use gamification to motivate your staff. For example, issue prizes when staff remember to sign out of their workstations or when they report a suspicious email. Also consider mock breaches that reward the practice for following your incident response plan during a fake phishing campaign.

How to Respond to the Worst-Case Scenario

"If you think your practice might have been hacked, don't panic," said Ms. Maldonado. "Take a breath and pull up your incident response plan. You put this in place and practiced the fire drill for a reason." With that plan in hand, you know which internal and external security experts to contact; how to determine the cause of the incident; how to respond to any ransom demands; how to seek legal counsel; and how to communicate a possible breach to your employees, your patients, and the public if need be.

Don't assume every incident is a reportable breach. "Treat everything as an incident until you know for certain that it's a breach," said Mr. Daigrepont. "An incident is not a breach. So get a second opinion because I've seen many practices overreact to simple incidents that are quite common."

For example, one of his clients reported a lost laptop to the Office of Civil Rights (OCR) even though, by law, the practice had 60 days to investigate the incident before reporting it. Although they eventually found the device within that time frame, the mere report triggered a larger investigation by the OCR. "This became a cascading scenario," he said. "When it was discovered that the laptop lacked any encryption, the OCR conducted a deeper audit and found that the practice hadn't followed through with any items in its SRA." Hundreds of thousands of dollars later, said Mr. Daigrepont, the practice ended up paying a high price for a simple incident.

Take each incident seriously. "As Warren Buffet reminds us, 'It takes 20 years to build a reputation and 5 minutes to ruin it,'" said Dr. Bovelle.

1 www.hhs.gov/sites/default/files/2021-hph-cybersecurity-forecast.pdf. Accessed Oct. 18, 2022.
2 www.wsj.com/articles/data-breaches-at-hospitals-associated-with-thousands-of-additional-patient-deaths-1521752610. Accessed Oct. 18, 2022.
3 www.healthit.gov/topic/privacy-security-and-hipaa/security-risk-assessment-tool. Accessed Oct. 18, 2022.
4 www.beckershospitalreview.com/cybersecurity/american-medical-collection-agency-reaches-40-state-settlement-for-data-breach-that-exposed-21-million-patients-info.html. Accessed Oct. 18, 2022.

Dr. Bovelle is in private practice in Glenn Dale, Md., and is director of cornea at Howard University Hospital in Washington, D.C. *Relevant financial disclosures: None.*
Mr. Daigrepont is senior vice president at the Coker Group in Atlanta. *Relevant financial disclosures: Coker Group: E.*
Ms. Maldonado is senior vice president at the Coker Group and CEO at Proda Technology, both in Atlanta. *Relevant financial disclosures: Coker Group: E, Proda Technology: E.*
See the disclosure key, page 8.

MORE ONLINE. Some hackers are targeting small practices. To find out why (and also to see who is on the HHS "wall of shame") read this article at aao.org/eyenet.