April 26, 2021 | Volume 35, Issue 17

Part B News
partbnews.com
COLLECT EVERY DOLLAR YOUR PRACTICE DESERVES

In this issue

decisionhealth
an hcpro brand

Health IT

Ransomware wrought havoc in 2020; sharpen tools, watch vendors to avoid breaches

In a bad year for the security of medical records, 2020 saw ransomware infiltrate more medical practices and cause more damage than ever before. Now's the time to review your vulnerabilities and consider upping your cybersecurity game.

For years now, businesses of all kinds, including medical practices, have been getting hit by hackers, who lock up their systems and demand a ransom to release them (*PBN 5/4/15*). Since then, the malefactors have gotten more sophisticated, hundreds of health care entities have been hit and millions of patient records have been compromised.

In 2020, cyber firms noted an uptick in ransomware attacks. The "Breach Barometer" of health care IT company Protenus in Baltimore saw a 42% increase in such incidents. A survey by UK-based international IT company Comparitech counted 92 ransomware attacks involving health care, some of them with far-reaching impact. All told, ransomware compromised 12.3 million patient records in 2020, according to Comparitech findings.

Because the HHS Office for Civil Rights has ruled that ransomware attacks are a breach under HIPAA, that's very bad news for the custodians of those records (*PBN 8/8/16*).

Even worse, "as Comparitech noted, its numbers are based on publicly reported breaches, meaning it includes breaches impacting more than 500 people and other breaches as reported in the media," says India Vincent, chief privacy officer and chair of the intellectual property, data privacy and cybersecurity practice group at Burr & Forman LLP in

Birmingham, Ala. "Attacks with fewer than 500 victims can often go unreported, or at least do not receive the attention necessary for the breach to make it into this type of analysis."

New dangers lurk

Experts who spoke to *Part B News* agree that ransomware is a bigger problem for practices now. For one thing, hackers know medical practices value their highly sensitive data and are more likely to pay that many other businesses, says Gary Salman, CEO of Black Talon Security in Katonah, N.Y. "In the hacking community, money talks," he says.

Experts also point to some new wrinkles that can make a ransomware attack especially painful. For example, more attackers are performing "double extortion" — that is, in addition to locking and ransoming your system, they steal some of your sensitive data and hold it for a separate ransom.

Sue C. Friedberg, a shareholder and co-chair of the cybersecurity and data privacy group at Buchanan, Ingersoll & Rooney in Pittsburgh, says that this, or part of it, has been happening for years. "It used to be referred to as a 'parting gift,'" she says. But "what's new is that [the hackers] will threaten to post the data on extortion sites," Friedberg adds. "They'll not only take the data but also actually expose it if the company refuses to pay the ransom."

Also, in addition to the usual phishing means of accessing systems — that is, using emails posing as legitimate business to tempt users into clicking links and downloading malicious code — more hackers are attacking systems directly by trying endpoints, such as server message block (SMB) ports, and muscling their way in.

"In the last three to 12 months, I would say the big exploits we've been seen have been the bad guys scanning firewalls that have known vulnerabilities," says Oli Thordarson, president and CEO of Alvaka Networks in Irvine, Calif.

In another new development, hackers are looking for copies of their target's cyber liability insurance policy that they'll actually use that against the organization, Salman observes. That's the hackers' way of saying, "By the way, you said you couldn't pay, but we see you have a half-million-dollar a policy, so we know you can," he adds.

Is paying ransoms illegal?

In October, the U.S. Treasury Department's Office of Foreign Assets Control (OFAC) issued a memo reminding businesses that "facilitating a ransomware payment that is demanded as a result of malicious cyber activities may enable criminals and adversaries with a sanctions nexus to profit and advance their illicit aims," and that paying ransoms that benefit certain international criminal organizations or known enemies of the United States could lead to sanctions.

decisionhealth an hcpro brand

SUBSCRIBER INFORMATION

Have questions on a story? Call or email us.

***PART B NEWS* TEAM**

Maria Tsigas, x6023
Product Director
mtsigas@decisionhealth.com

Marci Geipe, x6022
Senior Manager, Product and Content
mgeipe@simplifycompliance.com

Richard Scott, 267-758-2404
Content Manager
rscott@decisionhealth.com

Roy Edroso, x6031
Editor
redroso@decisionhealth.com

Julia Kyles
Editor
jkyles@decisionhealth.com

Medical Practice & Hospital community!

www.facebook.com/DecisionHealthPAC
www.twitter.com/DH_MedPractice
www.linkedin.com/groups/12003710

SUBSCRIPTIONS
Direct questions about newsletter delivery and account status, toll free, to 1-855-CALL-DH1 or email: customer@decisionhealth.com

DECISIONHEALTH PLEDGE OF INDEPENDENCE:
Part B News works for only you, the provider. We are not affiliated with any special interest groups, nor owned by any entity with a conflicting stake in the health care industry. For nearly three decades, we've been independently watching out for the financial health of health care providers and we'll be there for you and your peers for decades to come.

CONNECT WITH US
Visit us online at: www.partbnews.com.

CEUS
Direct questions about newsletter delivery and account status, toll free, to 1-855-CALL-DH1 or email customer@decisionhealth.com.

ADVERTISING
To inquire about advertising in *Part B News*, call 1-855-CALL-DH1.

Part B News® is a registered trademark of DecisionHealth. Part B News is published 48 times/year by DecisionHealth, 100 Winners Circle, Suite 300, Brentwood, TN 37027. ISSN 0893-8121. pbncustomer@decisionhealth.com Price: $647/year.

decisionhealth an hcpro brand

"Obviously, [the OFAC memo] is a worry because the government is basically saying payment of ransom is potentially a criminal act," says Eric B. Levine, executive vice president and shareholder, Lindabury, McCormick, Estabrook & Cooper PC in Westfield, N.J. "And the FBI has taken that position for a while."

But Levine has never seen anyone prosecuted for paying ransoms. "While it's probably legally viable, it's not really practical, particularly in health care," Levine says, because failure to pay may have "significant and immediate consequences" for patients.

In fact, Levine notes that both federal and state agencies have sections that can actually help parties hit by ransomware. In New Jersey, for example, the state Cybersecurity and Communications Integration Cell "keeps a list of known ransomware keys, and they normally have a pretty good success rate — somewhere about 50% have decryption keys," Levine says. If the hacker is just using an existing kit, as many unsophisticated ones do, the Cell may be able to unlock it for you.

New security tools

"Traditionally, the protection against ransomware was having a good reliable backup," says Greg Kelley, chief technology officer of Vestige Digital Investigations in North Royalton, Ohio. "If one got hit with ransomware, the backup would allow the company to get back up and going without paying a ransom. [But] now that the hackers are threatening to expose the data stolen, it is even more important to stop ransomware before it starts."

"Most small- and medium-sized health care entities are relying on in-house IT folks or an IT company for security, and often they don't really understand the threat landscape and they don't have the proper types of tools and knowledge to protect the data," Salman says. "So they're still relying on firewalls and anti-virus software and being, quote-unquote, HIPAA-compliant."

Salman suggests an investment in higher level security tools, such as endpoint detection and response (EDR) that "utilizes artificial intelligence and machine learning to make decisions as to whether or not a piece of code on the computer is malicious or not." Unlike lower-end anti-virus tools that work from a dictionary of known malicious files, an EDR "knows what malicious code and hacking tools typically look like," Salman says. "Even if the hackers think they're going to be slick and just kind of change the name on a piece of malicious code, it's still going to check it out and block it."

Thordarson recommends vulnerability assessments and penetration testing to find the weak spots in your systems.

Vincent advises you to mind your vendors, whose access points with your system may turn out to be its weakest links. "Many of the recent breaches have highlighted the importance of ensuring that the organization's vendors are following proper security measures in order to maintain the organization's information," Vincent says. "It may be difficult for many smaller organizations to implement a robust vendor management system, but having a checklist of key security measures all vendors are required to comply with can be a good start and help avoid some of the more preventable attacks."

Nothing like good training

It remains vital that you continue to perform the usual security precautions — for example, timely software and server patches and frequent backups that are segregated from the main server (*PBN 11/19/20*). As more elements of medical care, such as medical devices, come online, you are advised to secure all of your endpoints.

"If it's connected, it's vulnerable," says Christian Espinosa, managing director of Cerberus Sentinel of O'Fallon, Ill.

One of your best bets still remains to train your staff to recognize and reject phishing emails, experts say.

"I continue to see phishing emails, and many have been geared toward acquiring pandemic subjects like PPE, for example, or the vaccine," notes Pamela E. Hepp, a shareholder and co-chair of the cybersecurity and data privacy group at Buchanan, Ingersoll & Rooney.

Levine advises ongoing training. Recently, "I got an email from one of our support staff who basically said, 'Hey, I got this email this morning, I almost clicked on the link, what do you think?'" Levine shares. "And It was clearly a phishing email. The good thing was her training kicked in and she didn't click on the link. So we notified our IT department and immediately sent out an alert to all of our employees … Probably the best thing that everybody can do is continue employee training." — *Roy Edroso* (*redroso@decisionhealth.com*) ■

RESOURCE

- U.S Treasury "Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments," Oct. 1, 2020: *https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf*