4 CRITICAL STEPS TO PROTECT AGAINST RANSOMWARE

Don’t Let Your Practice Fall Victim to Hackers

Medical Economics®

nextgen® healthcare

TABLE OF CONTENTS

Train your staff to recognize phishing 3

Create an incident response plan 4

Secure all medical devices, not just computers 6

Move to the cloud for additional security 8

Conclusion 9

Put your plan to use: What to do if hackers strike 10

Cyberthreats in healthcare have grown dramatically in recent years. In 2020, the number of ransomware attempts against the healthcare industry rose by 123%, according to the 2021 SonicWall Cyber Threat Report[1]. Ambulatory medical practices are at risk from cybercriminals looking for easy targets — even though attacks on large health care systems are more likely to generate headlines.

Without the right cyber defenses, physicians may find themselves with no access to critical patient records. The long road to normal operations can financially cripple the practice for years or even force it to go out of business.

Physicians and other healthcare leaders can minimize the risks of cybercrime with these four critical steps.

[1] https://www.sonicwall.com/resources/white-papers/2021-sonicwall-cyber-threat-report

Medical Economics

1

Train your staff to recognize phishing

Email is the most common way ransomware invades computer systems. It happens when employees carelessly click on links in emails.

"Employees are typically the weakest link in any security program," says David Slazyk, chief information and security officer at NextGen Healthcare. "Building a culture of security in an organization is critically important but should be based around education versus punishment."

Make it experiential

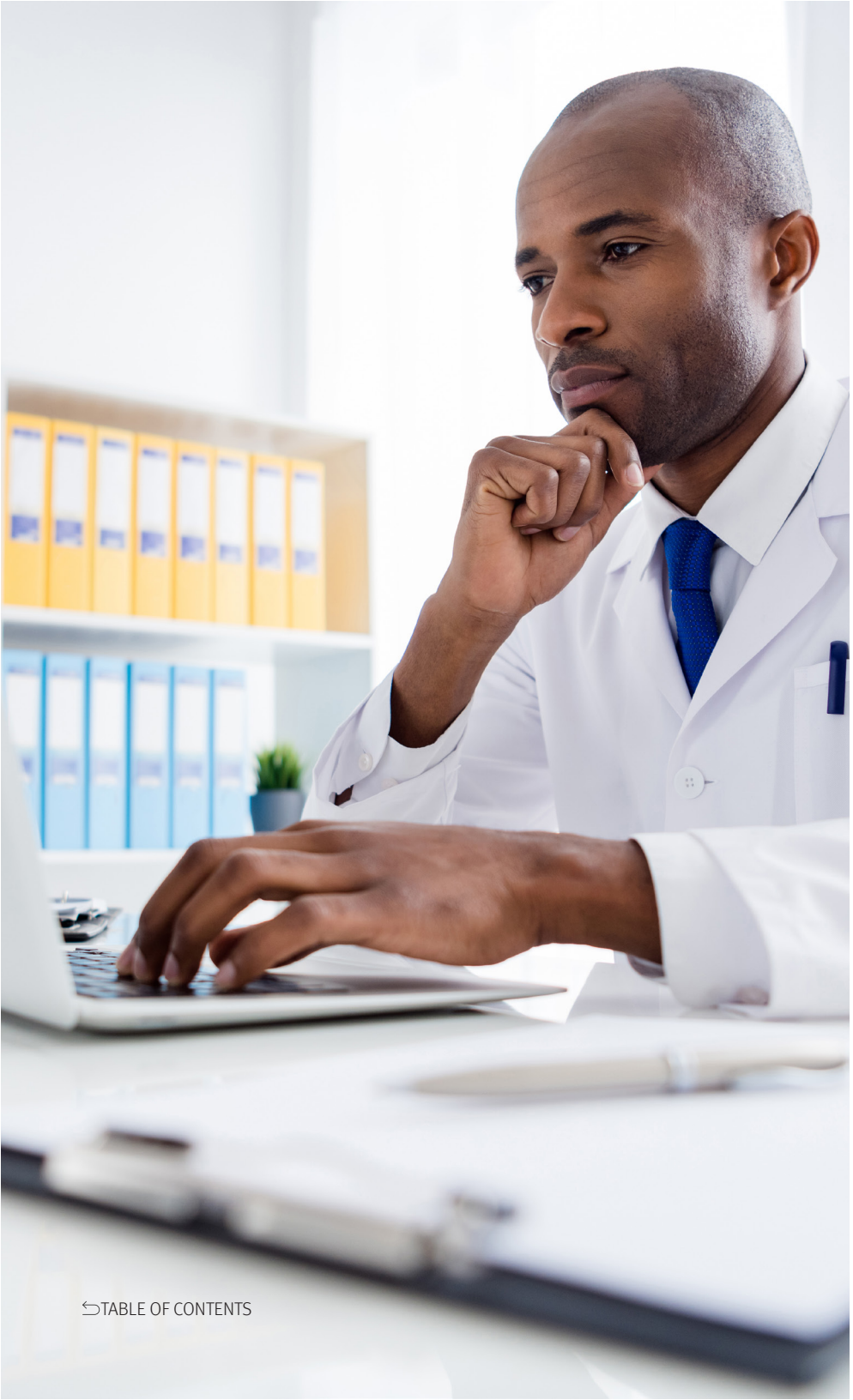
The most effective training is experiential, whereby employees are sent suspicious emails that mimic common phishing emails. If they click on the embedded links, they learn what they did wrong. Over time, the emails resemble highly targeted attacks known as "spear phishing" that appear to come from a boss or colleague. They even include company logos or information to make them appear official.

"It's not about sitting in front of a computer screen watching a PowerPoint training session," says Slazyk. "It's training that builds muscle memory for employees to say, 'This doesn't look right.'"

Training prevents intrusions

Rahul Telang, Ph.D., professor of information systems and management at Carnegie Mellon University in Pittsburgh, says training is vital to prevent intrusions. "Every small firm needs some sort of training program, beginning with when they start and then every six months after that," says Telang.

In addition to testing employees with simulated phishing attacks, Telang says because attacks are more common on public email services, employees should be encouraged to only access their personal email on their own devices, not from their work computers. A separate guest network for personal devices can further insulate a practice from hackers.



2

Create an incident response plan

An incident response plan outlines how a practice will respond to a cyberattack. It's similar to a fire evacuation plan. Hopefully, it's never needed, but every practice needs to have one. Slazyk recommends a dedicated playbook for ransomware attacks because of the complicated legal and technological issues that need to be considered.

For example, in the event of a cyberattack, was any personally identifiable health data viewed or exfiltrated from the servers? Only an information technology (IT) security expert will be able to answer this question. If so, then the federal government will need to be notified of the breach. The incident response plan should designate the practice's IT security experts in advance of any possible cyberattack.

"You want to have those relationships in place so you can reach out to the IT experts immediately versus spending three days trying to get a business relationship in place with a firm during a catastrophe," says Daniel Emig, vice president of hosting cloud technology at NextGen Healthcare.

To pay, or not to pay, the ransom

A practice also must consider whether to pay the ransom. If it's being paid, the recipient needs to be identified by country, lest the practice runs afoul of sanctions imposed by the U.S. government. For example, paying ransom to an organization based in a country under U.S. sanctions can create legal problems. "There are a lot of nuances around responding to ransomware, which is why a dedicated playbook is key in this type of threat," says Slazyk.

Keep the plan simple

Santiago Torres-Arias, assistant professor of electrical and computer engineering at Purdue University in West Lafayette, Indiana, says the incident response plan doesn't have to be overly complicated. It needs to have a clear timeline that addresses the following:

- Who should be notified of the attack (which might include a cyber insurance provider)?
- What experts should be brought in?
- What immediate steps should be taken to minimize the damage?

Where you keep the backup files matters

The plan should cover details on file backups and rebuilding databases.

"Make sure backup files are in a place where they won't get encrypted. Ransomware will encrypt everything on the drives at the primary site," says Emig. "The incident response plan also needs to include plans for rebuilding the servers and name who is responsible. Because ransomware hides everywhere on the system, you can't just restore data onto the existing servers."

Before practice operations can resume, all software will need to be reinstalled and all malicious code removed.

“Having more connected devices creates more vulnerabilities.”

Rahul Telang, Ph.D.
Professor of Information Systems and Management
Carnegie Mellon University

3

Secure all medical devices, not just computers

Technology is pervasive in all areas of health care; however, the convenience of high-tech devices also comes with a downside – they can be used as entry points by hackers into a practice’s computer system.

“Having more connected devices creates more vulnerabilities,” says Telang.

As a result, a practice needs to make sure all devices are secure, not just computers. “You want all computer-based clinical devices contained within your network, just like you would all your workstations,” says Emig. “Make sure that any internet traffic to or from clinical devices is going through your front-end defenses — firewalls, intrusion detection, and intrusion prevention. Make sure those devices go through system defenses and are not isolated on the network sending direct connections out into the web.”

Simple devices often overlooked

Medical devices can be overlooked by office staff. For example, a device in an exam room that uploads information to the internet is still part of the practice's network.

"Ask the medical device vendor what they are doing to ensure that these devices are regularly updated and maintained," says Emig.

Similar to a computer, these devices have patches available to fix known security flaws; however, if no one applies these patches, it can create an opening for hackers to exploit.

4

Move to the cloud for additional security

A cloud-based health IT solution offers ambulatory practices significant security advantages. Cloud-hosting services typically include security experts, and these systems are designed to keep intruders out.

"Being in the cloud offers more safety as well as an important backup location, as long as the cloud-hosting provider is reputable," says David Nicol, Ph.D., professor of electrical and computer engineering at the University of Illinois at Urbana-Champaign and director of the Information Trust Institute. Denial of access to your data after a ransomware attack is more severe on a local computer that is self-hosted. On the other hand, if your data is in the cloud, you can still be denied access, but you'll be able to get a recent backup.

Hacking the cloud is more difficult

Cloud providers offer world-class tools that help protect data from attacks.

"A lot of security protections come native to the cloud environment," says Slazyk. Cloud providers have access to more bandwidth, which makes it easier to do secure backups. Data can be backed up to a different geographic location more frequently. If ransomware strikes the medical practice, only a small amount of data is lost, and the system rebuild can begin almost immediately.

"Within the cloud, there are protections that help contain the spread of ransomware," says Slazyk. "These are sophisticated, expensive tools for individual practices to purchase but exist natively within the cloud."

Look for third-party security validation

Third-party certification ensures a vendor follows best practices for data security. HITRUST is one such designation, and to earn it, companies must comply with hundreds of security controls and regular audits. A cloud provider with HITRUST operates at the highest security levels in the industry.

TABLE OF CONTENTS

Conclusion

The number of ransomware attacks in health care has been increasing for years. Unfortunately, this trend is expected to continue.

To set up protective measures against an attack, ambulatory practices should:

- Train staff to recognize deceptive emails that allow hackers to access a practice's computers
- Have an incident response plan ready to respond to a data breach quickly
- Be aware that connected medical devices can be vulnerable to hackers who can bypass firewalls and other security measures
- Move their data to the cloud to boost overall security and reduce recovery times

If practices do not protect themselves, a ransomware attack can be disastrous. However, the right plan can help a practice be up and running in a matter of hours or days instead of weeks or months.

"Within the cloud, there are protections that can help contain the spread of ransomware."

David Slazyk
Chief Information and Security Officer
NextGen Healthcare

Put your plan to use: What to do if hackers strike

Recognize the attack

The first sign a practice has been hit with a ransomware attack will most likely be a locked computer screen with a message that indicates that all its files have been encrypted along with an email address to contact the hackers to arrange ransom payment.

Shut everything down

"If it happens, shut everything down, don't even blink," says Emig. "I can't emphasize this enough because every minute that passes, it is propagating itself deeper in your system."

Notify leadership

Next, notify all members of leadership as well as the insurance provider (if the practice has cyber insurance) because it may have its own specific steps that need to be followed.

Assemble your team

Emig recommends lining up available resources, whether it's an internal information technology (IT) team or a third-party provider. "The practice has to start over, and they need to rapidly implement the plan on how they are going to rebuild the servers and restore the backups," says Emig.

Remain calm and consider your options

Slazyk says it's important to stay composed and think rationally during the crisis. "You don't want to just quickly decide to pay the ransom and try to make it go away," he says.

Part of the reason for that is because malware can take time to get into a system and activate. The hacker group that created it may have been shut down in the interim, and any ransom sent into cyberspace may be for naught.

Determine whether to notify patients

Another major decision for practices hit with ransomware is whether to inform patients about the attack. “That’s determined by whether the data was encrypted in place or encrypted and extracted,” says Emig. This detail will need to be assessed by an IT security expert, and the practice needs to move quickly.

“The minute you see the ransom message on your screen, the clock starts ticking, and you have 60 days to report to (the U.S. Department of Health & Human Services) whether it was a breach or not,” says Slazyk. If the files were encrypted but not removed, it probably would not be considered a breach, but legal counsel will need to be brought in to make a final determination. Usually, patients do not need to be notified by the practice if it’s not a breach. Still, the practice needs a communication plan if patients ask for information about their files before backups can be used to rebuild the servers.

Estimate your recovery time

Recovery time varies by how much data is locked by the ransomware and the quality of the practice’s backups. With a detailed incident response plan, solid cloud-based backups, and an experienced IT team, a practice might be back to normal in a matter of hours or a day or two. In complicated cases, it might stretch to a week.

“If you haven’t taken any precautions and if you don’t have a reliable backup, then you are talking about a recovery time that could take weeks, months, or maybe never,” says Slazyk.

BETTER STARTS HERE.

Contact us at 855-510-6398 or results@nextgen.com

Learn how NextGen® Managed Cloud Services can help your practice meet today's health IT challenges and reduce your costs.

CO_121421_4CriticalStepsAgainstRansomware

Medical Economics®

nextgen® healthcare