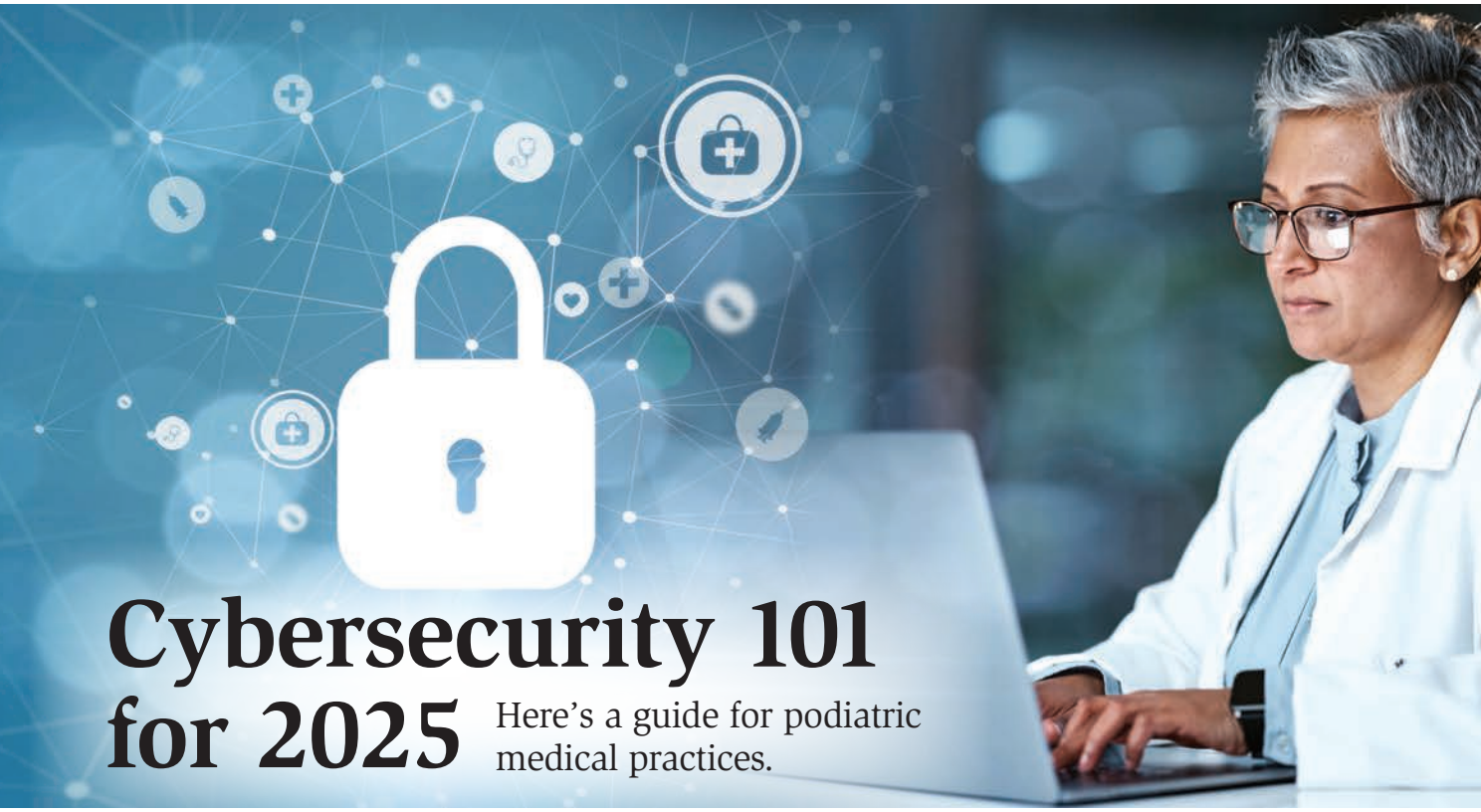

Cybersecurity 101 for 2025

Here's a guide for podiatric medical practices.

BY MARK TERRY

The Internet is a reflection of the world. It has great diversity and many beautiful things in it. It also has bad neighborhoods, criminals, and predators. Unlike in the real world, where criminals and predators typically have to be in proximity, the Internet puts any criminal and predator at your front door, if they want to be there. And the criminals and predators do view healthcare facilities, from individual practices to major health systems, as juicy targets.

"That's the reality of the Internet and being part of this interconnected world," says Errol S. Weiss, Chief Security Officer of Health-ISAC. "Unfortunately, the threats can come from literally anywhere. And they do."

ISAC stands for Information Sharing and Analysis Center. In the mid-1990s, the federal government conducted a study looking at cybersecurity and resilience across all the critical infrastructures, such as finance, transportation, energy, healthcare, etc. Finding that much of the critical infrastructure was owned and operated by the private sector, the government encouraged the creation of ISACs for each critical infrastructure to work with each other and share threat information. There is at least one ISAC for each critical infrastructure.

Unlike in the real world, where criminals and predators typically have to be in proximity, the Internet puts any criminal and predator at your front door, if they want to be there.

Weiss says, "It's really like a virtual neighborhood watch program. The whole idea is that you see something happening in the neighborhood that looks a little suspicious, or something's happening and you want to help other neighbors. There's a community and network of trust to share information."

Unfortunately, Weiss says that what they're seeing related to small medical practices is "computers that have been taken over by malware or they've been targeted by ransomware groups and their systems are literally held hostage until they pay a ransom. And even worse these days, we've seen criminal gangs getting into medical networks. They're encrypting the systems so they become inoperable for that practice. And even worse yet, they've actually stolen a copy of all the data there and if you don't pay the ransom, they will threaten to release that data."

Here are just a few examples of recent attacks:

• Lehigh Valley Health Network in Pennsylvania was the victim of a Feb-

Continued on page 74

Cybersecurity (from page 73)

ruary 2023 ransomware attack when hackers posted nude photographs of cancer patients online after the health system refused to pay the ransom. In September 2024, the healthcare system agreed to pay $65 million to the victims.

• In July 2024, UnitedHealth Group's Change Healthcare suffered the most significant cyberattack in American history, costing the group more than $3.3 billion. Part of the fallout was that United was unable to process medical insurance submissions for patient care and payments to medical practices. Some medical offices found themselves unable to receive payments for weeks.

• In September 2024, Boston Children's Health Physicians, which pairs children with more than 300 physicians through 60 regional offices as part of the Boston Children's Hospital network, suffered a breach with hackers stealing files that contained patient data like Social Security numbers, addresses, medical record numbers, health insurance and billing data, and treatment information.

Although the biggest news stories have focused on health system attacks (which in many cases also affected affiliated medical practices), medical offices can also be the target of attacks.

Michael Brody, DPM, of Long Island Podiatry Services as well as Founder of TLD Systems, a company that assists practices in compliance with HIPAA and the HITECH Act, says, "In addition to worrying about your computers and your antivirus and encryption, now you have to start worrying about what else is connecting to the network that will allow someone to break into your office and steal your data."

Brody adds, "Under the federal government rules and regulations, patients have a civil right to their information being kept private and secure. Failure to do your due diligence to protect your patient records is a violation of their civil rights, which is investigated by the Office of Civil Rights, which is a division of the Department of Health and Human Services (HHS). You have an obligation to keep their information private and secure, the same way you want other people to keep your information private and secure."

As Brody notes, how your practice's computers, phones, and digital instrumentation connect to the Internet can be a vulnerability.

4 Key Vulnerabilities

There are (at least) 4 key cyber vulnerabilities:

1) Your network. As Brody notes, how your practice's computers, phones, and digital instrumentation connect to the Internet can be a vulnerability. This can broadly include organizational processes, hardware, or software. The most common vulnerabilities in networks include:

• Misconfigured firewalls or operating systems.

• Malware. This is any form of malicious software installed on a host server or user's device.

• Unpatched or outdated software.

• Social engineering or so-called "Phishing" attacks. This is where users are tricked into providing information, such as their username and password. Cybercriminals are increasingly using artificial intelligence (AI) for even more sophisticated and difficult-to-detect attacks.

• Credential stuffing. This is when cybercriminals use data they've

Continued on page 76

Thoughts on Ransomware

According to a 2021 global survey conducted by the United Nations, more than one-third of healthcare institutions that responded reported at least one ransomware attack the previous year and a third said they paid the ransom. [https://news.un.org/en/story/2024/11/1156751] A ransomware attack is a type of cyberattack where the criminal takes over or locks files on a computer or network and demands payment for returning access.

In a 2024 statement, World Health Organization (WHO) Director-General Tedros Adhanom Ghebreyesus noted, "At best, these attacks cause disruption and financial loss. At worst, they undermine trust in the health systems on which people depend, and even cause patient harm and death."

Brody points out that paying ransomware "is problematic because often these criminals are from areas that have been designated as terrorist organizations and sending money to such an organization is a violation of Department of Justice rules. So paying it could create legal problems above and beyond paying the ransomware."

And, of course, paying it doesn't guarantee they won't just keep upping the ransom while never resolving the attack.

Brody warns, "If you are hit with a ransomware attack, do not try to fix this yourself. Ransomware is considered a breach of data unless proven otherwise because a foreign process has accessed your data to encrypt it. How do you know that that foreign process doesn't still exist in your system? You need a forensic specialist to go through your network and routers to check your log files and demonstrate that the software that was used to encrypt it didn't send another copy off-site. Bring in qualified professionals who can do a forensic analysis to determine what happened, how it happened, and determine if you were actually breached or you just had your data encrypted." **PM**

Cybersecurity (from page 74)

collected from a previous breach to break into more user accounts.

2) Operating systems. These are where hackers try to gain access to an operating system (OS). There are many different ways these are exploited, including denial-of-service (DoS) that can be "flood attacks" where the system receives a barrage of requests, resulting in it slowing down or halting, or "crash attacks" that exploit vulnerabilities to cause a system or service to crash. Others include "information disclosure" attacks where hackers steal personal data and disclose it, and "spoofing" where the criminal impersonates someone with higher level access.

3) People. It only takes one person within a practice or health system to click on the wrong email link, make their network access username or password be accessed, or maliciously attack a system from inside to make the entire network and practice vulnerable.

4) Process vulnerabilities. This is a broad category but includes things like processes that allow users to create weak passwords, don't insist on regular changes in passwords, and don't require multifactor authentication (MFA). It would also include users not logging out after use and/or multiple people using the same devices without having to log in or out.

10 Steps for Medical Practice Cyber Hygiene

Every year, technology gets a little bit better at fending off cyberattacks. Unfortunately, cybercriminals adapt and get more sophisticated and creative. They also are utilizing AI to help design cyber-attacks.

Weiss says, "Essentially, these criminal gangs don't care where they get the money. They are just out to raise cash, and they will go to any length to achieve that goal. If cybercriminal gangs can gain hold of even a small practice and get a few thousand medical records and try to extort thousands of dollars from that practice, or tens of thousands of dollars from that practice, they will try to do that."

Here are 10 steps for good cyber hygiene:

1) "First," Weiss said, "***make sure you're keeping your systems up-to-date***. The Windows and Apple systems today are doing a much better job of keeping themselves up-to-date automatically on a regular basis. But I would want to make sure that older systems or legacy systems attached to your network are getting regular updates on all patches, etc."

2) The second, Weiss says, "is to ***back up the systems regularly and make sure that those backups are working.*** Test them occasionally and make sure what's backed up is what you intended to be backed up and that you can actually retrieve files from those backups."

Weiss notes that most of the online, cloud-based backups available today are what he calls "set and forget," and they're reasonably reliable. If something should happen to your facility or the computers in it, most of your data should be salvageable.

3) The third is ***multifactor authentication.*** "If you have any connection to the Internet," Weiss says, "es-

Continued on page 77

Cybersecurity (from page 76)

pecially if you're doing remote access and logging in after hours from home, checking on things or on patient records, you have to use multifactor authentication: username, password plus some token. There are really good authentication systems out there, very simple and inexpensive to implement."

4) When possible, ***use encryption.*** Brody notes that 10 years ago, the software to encrypt your hard drives was expensive and technically difficult. "It was beyond the resources of a small provider. Now encryption is inexpensive. BitLocker is built into most Windows computers. There is no reason why your computers are not encrypted today."

5) ***Robust firewall and anti-malware software.*** Common providers that offer affordable and fairly easy-to-use products and licensing for multiple devices include Bitdefender, McAfee and Norton, to name the biggest players on the market.

Emphasize the importance of cybersecurity for all staff and conduct regular training and reminders.

6) ***Implement user access management.*** As mentioned under the "People" category, each person using the system needs their own login. The practice should keep and update a list of staffers who can access each software or program. People who leave the practice, or for whatever reason no longer have access, need to be removed from the list and their access changed.

7) ***Train and retrain staff regularly.*** Emphasize the importance of cybersecurity for all staff and conduct regular training and reminders. If processes or software are added or changed, train staff on appropriate usage and cybersecurity.

8) ***Manage vendors and vendor access.*** Sometimes the data leaks come from outside your practice. When working with vendors, ask about their security practices.

9) ***Develop a backup and recovery plan.*** Do you have a plan for handling the catastrophic loss of patient data, whether through disasters such as fire, flood, earthquake, or cyberattacks? Create a comprehensive backup and recovery plan. Ensure critical data is backed up and stored securely off-site or in the cloud. Test your backup and recovery processes regularly.

Brody says, "The best defense against ransomware is a good backup. You simply wipe your systems, reload them, and restore your backup; and you are back up and online and you've only lost a few hours."

10) ***Invest in cybersecurity insurance.*** If cyberattacks aren't included in your practice's insurance policies, look for coverage. Brody says everybody should have it. "The same reason you have homeowners' insurance. Do you expect your house to burn down? No. But if it does,

Continued on page 78

Cybersecurity (from page 77)

you want the insurance. It's the same thing with cybersecurity insurance."

It's a Nuisance

Constantly changing passwords, constantly updating operating systems, constantly training staff, constantly investing in antiviral, antimalware, and encryption software is a nuisance. Why bother?

"People also say that having to take courses to keep your license up-to-date to practice medicine is a nuisance," Brody says. "Yes, it's a nuisance. But if you don't keep up, you fall behind. Taking your car in for a regular oil change is a nuisance. So is a locked-up engine. Why do I have to do my laundry this week? I just did it last week. It's the nature of reality."

That said, what is "reasonable due diligence" for a podiatric practice? That's a much fairer and more difficult question. Luckily, the cost of technological solutions like antiviral software, encryption and cloud storage has come down significantly.

There is no one-size-fits-all solution for podiatry practices in terms of cybersecurity. Brody notes, "If you go into six different practices, you're going to find 66 different configurations of networks, another six different types of routers or firewalls. Some people buy their own; some people use one from the Internet provider. You can have some with the Internet of Things (devices connected to the Internet), and different types of software. Some will use Windows computers; you may have Apple computers, and you may have Linux computers. Some may use iPads or Android tablets. Every location is different."

As true as that is, there are best practices for all those solutions, which are described in the cyber hygiene section.

Brody says, "The resources and technology that's available to you today is greater than the resources and technology available to you a year ago. So if you're not changing things, you're not keeping up, because the threats out there today are greater than the threats of a year ago."

That said, for a medical practice, how much to spend and how much time to invest is a balancing act. You have to weigh the investment with the risks and potential fallout from those risks, which can be considerable. **PM**

Mark Terry is a freelance writer, editor, author and ghostwriter specializing in healthcare, medicine and biotechnology. He has written over 700 magazine and trade journal articles, 20 books, and dozens of white papers, market research reports and other materials. For more information, visit his websites: www.markterrywriter.com and www.markterrybooks.com.