of layers," he said. "It's like protecting your home. You have an automatic lock, and you back that up with a deadbolt. Then you add motion-sensitive lights and perhaps an alarm system. The idea is to get a thief to skip your house and go to a softer target."

Identifying vulnerabilities

A company's wireless network is an often-overlooked vulnerable point. "A sophisticated attacker may use Wireshark [a legitimate analytical tool that hackers sometimes use to reverse-engineer their way into a network], or they may start by just camping out in the parking lot of a business, like a law office or other professional services firm," according to Schober. "They may stop in or call a receptionist and say they've got to send a proposal to the CEO — mentioning his or her name to add legitimacy — and then ask for the wi-fi password. Boom, they're in and can infect the system with malware."

Staff also need to be educated about not blabbing too much on social media, he added. "Don't post things like 'here's where we're eating dinner, or where we went on vacation,' because those can all be pieces of a puzzle that help hackers to crack passwords," Schober warned.

Healthcare providers need virus protection

Hospitals and other healthcare providers have to be particularly careful about guarding their data from hackers, said Lani Dornfeld, a partner in the health law practice at Brach Eichler LLC. Civil fines under HIPAA, the Health Insurance Portability and Accountability Act of 1996, are bad enough — in 2018, health insurer Anthem Inc. paid a record $16 million fine to the U.S. Department of Health and Human Services' Office for Civil Rights, following a massive breach — but cyber-leaks may also expose a victimized company to criminal charges.


Dornfeld

"Under HIPAA, once you learn that you've been attacked and health information may have been accessed, you need to investigate as soon as possible," she counseled. "If the attacker didn't access sensitive data, you may be off the hook. But if the hacker did access data, the provider may have a duty to report the breach to a variety of parties and you could face civil penalties. Under federal regulation 42 CFR Part 2 [Substance Abuse Confidentiality Regulations], however, criminal charges may also be filed."

She's created a checklist, which includes pointers like assembling a response team as soon as possible — you should already have one mapped out — and keeping track of all relevant dates, along with a detailed journal or record of all actions, results and responses.

"Gather, protect and save your evidence, and take reactive and proactive measures," Dornfeld added, "in order to reduce fines and penalties, and protect against future attacks or incidents."

Another precautionary step is to check out the Dark Web — a part of the internet that's often used by criminals, which can only be accessed with certain software — to see if your personal information is available for sale. When companies like Target Corp. and Equifax suffered breaches and exposed millions of bits of sensitive customer data, "people eventually found out, but in some cases it took a year or more until they were notified," Schober said. "Business owners and others can use services like Cyberlitica, which scour the dark web, so they can get early warning and change their passwords and take other steps to protect their information."

Vincent Lagonigro — an IT services provider who works with the CPA firm Levine, Jacobs & Co. and other businesses — said using dual factor authentication for emails and other accounts "can take a little longer, but can make it more difficult to penetrate your system."

As a test, Lagonigro periodically sends out fake "phishing" emails — with bogus links that try to trick people into sharing valuable personal or company information — to client company employees, to see which ones take the bait. "We get a live report so we can see who's entering credentials on a fake site," he said. "It's all part of a training effort that incorporates human behavior as well as technology."

Other safeguards include Cisco Systems Inc.'s OpenDNS service, "Which can help prevent you from going to a site that may be hacked," Lagonigro added. "Just the other day, a new client that provides financial information, and uses the popular WordPress website platform, was hacked. People who tried to click on their site were redirected to potentially harmful sites. Fortunately, OpenDNS' zero hour response blocked it on a global basis almost immediately."

Hackers present multiple threats to small business owners and others. But companies that keep up to date with security measures and training have a better chance of staying safe.