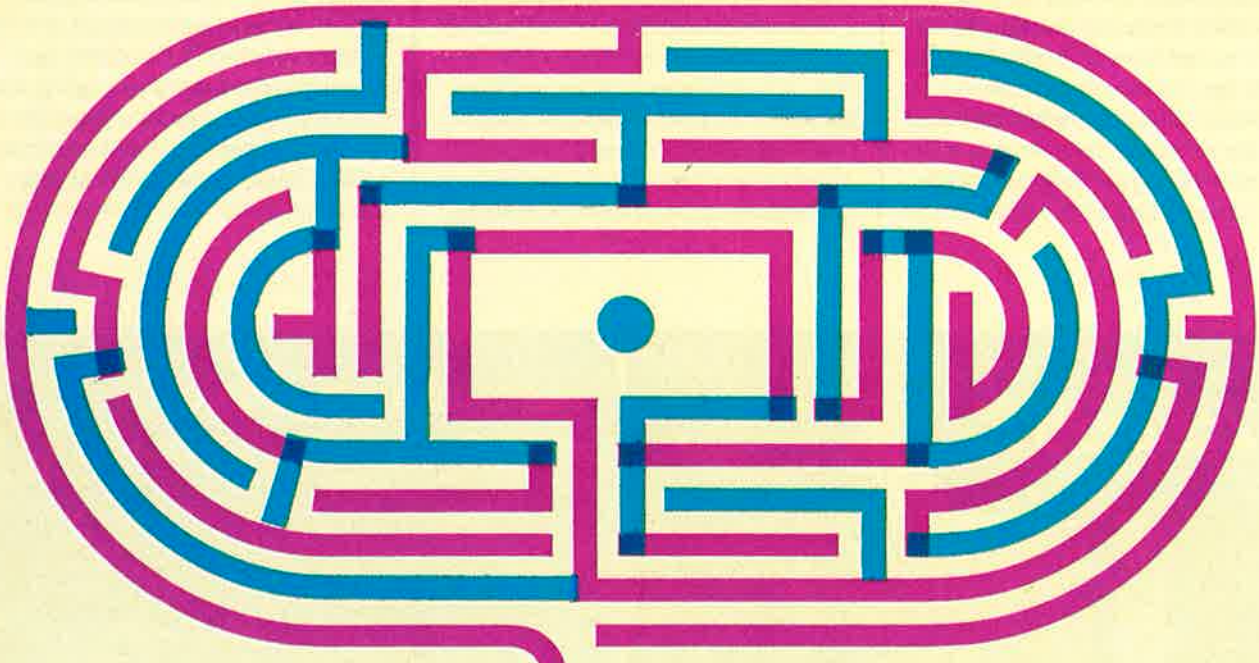
THE HACKER IN THE CLINIC



Why physicians have become targets of ransomware attacks and what you should know about it BY KYLIE TAGGART

RECENT YEARS HAVE seen some well-known cyber attacks on healthcare services. The most jaw-dropping was the 2017 WannaCry ransomware attack that hit the U.K.'s National Health Service. Access to patient files was blocked, appointments were cancelled and surgeries were postponed.

While most reports of healthcare cyber attacks involve hospitals, physician's offices and clinics in non-hospital settings are also vulnerable—even if we don't know precisely how often they are hacked.

Robert Beggs is the CEO of the Waterloo, Ont.-based cybersecurity company DigitalDefence. He has worked with a number of physician's offices after they've been hacked. He was unable to share details about the cases, but said he was working on one when the *Medical Post* spoke with him in mid-July.

Similarly, the Canadian Medical Protective Association (CMPA) wrote in 2017 that physicians had reported "ransomware incidents affecting their practices and EMR systems." This malware encrypts and locks files, and hackers then demand ransom to release them. The ransomware usually gets into the computer network when someone opens a file or link in an email.

It is estimated that less than 5% of victims report their case to the Canadian Anti-Fraud Centre (CAFC), Canada's central intake of data and intelligence concerning fraud. While the CAFC does not track data for physician's offices specifically, it did receive 141 complaints of fraud in the healthcare sector in 2018, down from 167 in 2017 and 173 in 2016. Of the 2018 complaints, 36 victims were bilked out of more than $2,390,000.

WHY DOCTORS ARE A POPULAR TARGET

Beggs said that the healthcare industry is a prime target for cybersecurity threats due to a trifecta of temptations for the hacker: healthcare offices hold personal information, financial information and, in some cases, intellectual property information.

Attacks can take many forms. Extortion (which would include ransomware) was the most common complaint from the healthcare sector to CAFC in 2018. Complaints were also made about directory fraud, identity fraud and spoofing, which is when a hacker mimics a trusted source to get the recipient to disclose information or allow access to a network. Healthcare complainants also reported being victims of spear phishing—a form of phishing that often mimics internal emails.

Physicians are a more attractive target than regular small businesses because the data they hold is more valuable to both the doctor and the patient. On the black market, an active credit card number is worth about $15, but a patient health record is worth about $1,000. Physicians are also considered to have a greater capacity, financially, to pay ransom.

WHAT HAPPENS IN AN ATTACK?

In a previous interview with the *Medical Post*, Beggs talked about one Canadian physician who was locked out of all their clinic's information, including scheduling. They had no idea who was going to walk into the office.

In a case like this, an attack would not only disrupt patient care, but it also leaves the physician liable for breach of privacy. This is true even though ransomware software doesn't give the hackers access to the data they've hacked—it only prevents the target from accessing it.

The dollar value of the ransom demanded by the hackers is not necessarily high. "For medical offices, they keep the ransom at $3,000 to $5,000—easy for a doctor to pay, but still profitable," Beggs said. For hospitals, the ransom is usually closer to $25,000.

Beggs told the *Medical Post* in 2017 that of four cases in 2015 where Toronto-area physicians' offices were hacked, three paid the ransom. The fourth was unable to recover the data.

New forms of ransomware are arising all the time. Some encrypted files can be recovered, but others cannot. Beggs referred to a new version of the malware called RKUY which encrypts information and, as of the time of the July 2019 interview, there was no known way to decrypt it.

MORE SOPHISTICATED TACTICS

Hackers are also changing tactics, Beggs said. For example, they might attack a system but not act on it for six months. By that time, if an office is backing up their files, the backup files will also be infected. When the victim reboots their system with their backup files, they don't realize those are infected as well.

There are also reports of wireless devices connected to the network being compromised; devices such as heart rate monitors and physicians' tablets. "Attackers are learning to compromise those more effectively," he said.

Health Canada recently recalled certain insulin pumps because they were vulnerable to cyber attacks. In the July 2019 press release, Health Canada noted that the pumps could be manipulated by someone who knew the serial number, had a nearby wireless connection, the correct radio frequency and, of course, malicious intent. Still, the risk was enough to merit a recall.

"The attack surface of the medical industry is increasing," Beggs said.

Physicians and their staff can also be victims of phishing, spear phishing or spoofing scams. For example, emails may look like they come from a trusted source but trick the recipient into giving away personal information or clicking on a file that installs malware. Some scams involve asking to pay a plausible-looking invoice through a wire transfer.

Ariane Siegel, general counsel and chief privacy officer at OntarioMD, said OntarioMD has received calls about phishing and similar issues.

"Just like everybody in the general community, physicians will be seeing the same phishing expeditions we all do, whether we are at work or at home," she said. OntarioMD supports physicians in the selection, implementation and adoption of EMRs and digital health tools.

EMR providers are constantly updating to prevent cybersecurity threats. OntarioMD has a robust EMR certification program, where companies must adhere to certain requirements, including privacy and security components, in order to obtain certification. "So far, we haven't got that many calls when it

Getty Images

comes to hacking EMR data, especially when it comes to certified EMRs," Siegel said.

HOW TO PROTECT YOURSELF

The biggest innovation in cybersecurity has been the cloud, Beggs said. Siegel said backups are fundamental to safeguarding health information. There are significant advantages to cloud-based storage, although there are still risks. For example, the data must be secure and encrypted both in the cloud and during transmission to the cloud, all while remaining readily accessible.

"One thing that can never be outsourced—and the privacy commissioner has been very outspoken about this—is accountability," Siegel said. "No matter where a physician's data is stored, whether it is a local EMR solution or a hosted one, it never removes the requirements for accountability."

Data protection is a shared responsibility among clinic staff, said Dr. Kathleen Ross, president of Doctors of BC and a family physician in Coquitlam, B.C. In the end, however, a patient's medical information is the responsibility of the physician.

Dr. Ross stressed that cybersecurity does not need to be difficult. The main point is training and education for all staff. "Once physicians understand that cybersecurity is something to be considered, it is really the biggest part of the battle," she said.

Dr. Ross suggested all offices should have a privacy policy, which includes cybersecurity, and regular auditing to make sure all staff are adhering to the policy. Physicians should also consider and plan how the office will function in the event of a cyber attack, and how any lost data will be recovered.

Doctors of BC has a number of resources for physicians on cybersecurity. Its Doctors Technology Office provides workshops. An online security course developed in partnership with the University of British Columbia is also scheduled to launch this fall.

OntarioMD worked with the CMPA and others to develop a free 45-minute security and privacy training module for physicians and staff. "When people ask me what is the number one thing we can do to protect your practice, training is always the answer," Siegel said.

Having reliable IT help is essential to preventing cybersecurity breaches. Beggs estimated that an evaluation by a cybersecurity expert in a single physician's office may cost $3,000 or less. The cost once a system is breached is significantly higher, he said.

A final tool for prevention is cyber insurance to cover losses in the event of a data breach. The Insurance Board of Canada told the *Medical Post* that this type of insurance is on the rise. A study by MSA Research, Inc. found that $92 million in premiums were paid by businesses in Canada for cyber attack coverage in 2018.

Patients need protection too. Dr. Ross even has a pamphlet for patients on how they can protect their personal information. After all, the stress of falling prey to a hack or scam is detrimental to good health. **MP**