Michigan Physicians' Practice Closes Its Doors After Hackers Erase All Data

When patients leave their healthcare provider's office, they may not stop to consider that they're leaving something behind. A yet, sensitive patient data is necessary for the running of the practitioner's business, even as it leaves patients vulnerable to s degree.

According to a report by specialist insurer Beazley that analyzed 2018 cybersecurity data, ransomware attackers target the healthcare industry more than any other. And those attacks are on the rise, with a spike in the final months of last year.

Unless you've been personally affected by a cybersecurity breach or attack, the consequences may sound more abstract than concrete. But a recent case in Michigan illustrates the potentially devastating results of fully executed hacking.

As reported by the news outlet WWMT West Michigan, Brookside Ear, Nose and Throat and Hearing Center will close after cybercriminals wiped out the entirety of the practice's patient files.

Physicians refuse ransom request; hackers wreak havo

Ransomware hackers ordered the practice to pay $6,500 to decrypt the IT system's fully encrypted files. The cybercriminals w met with flat refusal by John Bizon, MD, and William Scalf, MD, the co-owners and co-founders of Brookside ENT and Hearin Center, at which point the hackers completely razed the practice's digital landscape.

In addition to all of the patient records, all payment data and calendar and scheduling information was deleted. However, Bizo said that because the patient data remained encrypted, the cybercriminals were not able to access that sensitive information t use it for identity theft.

Faced with the daunting task of piecing the practice back together without a shred of information to get them going, Bizon and Scalf opted to retire from medicine ahead of schedule instead. Understandably, that's not a decision that sits well with all patie

A patient spoke with WWMT and reported finding out about the file erasure when she called the office to schedule a post-surg follow-up visit. Because the exact details of that particular surgery were contained in the now-deleted Brookside's records, the patient's new provider will not have the benefit of that medical history going forward. So although her data was not compromis a way that leaves her open to what we typically fear after a breach (thanks to the encrypted files), she faces unanticipated hur involving her future care, through no fault of her own.

The cybercriminals have not yet been apprehended, although the FBI is presently investigating the incident. Brookside's owne have said that they believe the ransomeware attack was limited to their practice.

Smaller practices seem particularly vulnerable

When it comes to ransomware attacks, cybercriminals prefer practices like Brookside ENT and Hearing Center — in other wo small-to-medium organizations, which are the subject of these types of attacks more than 70% of the time. And that's no acci

"Unfortunately, it's often smaller businesses that are most vulnerable to attack by cybercriminals as they frequently lack the resources and protocols of larger firms," Beazley Breach Response Services Head Katherine Keefe told HealthITSecurity whe the report was released. "Businesses of all sizes need to ensure their IT employees are aware of the risks through up-to-date training and implementation of cyber security measures."

Education is the key to prevention

Beazley reported that although accidental disclosure leading to data breaches dropped by more than 10% over the previous year, it still represented the most common cause of cyber-vulnerability. Malware and hacking jumped from 20% to 30% over the period of one year.

Naturally, cyber-attacks are not exclusive to healthcare; the report revealed that events involving compromised business emails spiked dramatically in 2018, and those attacks ensnared healthcare, finance, education, and various professional services.

In a statement following another cybersecurity report, Keefe said: “Unfortunately, we see these threats globally across all sectors, and we strongly believe that education about the risks and preparedness are as important as IT security measures for protecting individuals and assets from cyberattacks.”