THE
NATIONAL LAW REVIEW

Small Michigan Medical Practice To Close Following Ransomware Attack

jackson lewis.

Article By
Joseph J. Lazzarotti
Jackson Lewis P.C.
Workplace Privacy Blog

- Communications, Media & Internet
- Michigan

Tuesday, April 16, 2019

Small and midsized enterprises (SMEs) continue to be targeted by ransomware, phishing and other cyberattacks; the consequences of which could be devastating. Those consequences include putting SMEs out of business, which is unfortunately the case for one small medical practice in Battle Creek, Michigan, as reported by HIPAAJournal.

The reality is that the effects of these attacks could be significantly mitigated with a bit of planning. Just maintaining good backups can go a long way. Of course, there are a number of other steps that SMEs can take to more comprehensively defend against these attacks.

The reports about the Michigan practice explain that the malware encrypted the system that maintained patient records and that the owners refused the attacker's demands for payment. Refusing to pay these demands is not uncommon. The Federal Bureau of Investigation, which provides guidance on preventing ransomware attacks, does not encourage paying ransom. In some cases, ransomware attack victims have recovered their data after paying the ransom, however, there is no guarantee of that in a particular case. In fact, in some cases, after making the requested ransom payment, attackers have been known to request more money to unlock the data. Note also that payments of ransom to persons or entities on a U.S. Department of the Treasury's Office of Foreign Assets Control ("OFAC") sanction list could be prosecuted.

When the Battle Creek physicians did not succumb to demands for payment, the attackers deleted all of the encrypted files. Reports indicate that no patient data

had been accessed or exfiltrated (removed) from the practice's systems, however, some patients may have lost all or a portion of their medical records. The practice is schedule to close at the end of this month.

SMEs certainly can improve their defenses to prevent and minimize the effects of an attack, however, they also need to be prepared to respond to an attack when it happens. Maintaining a written incident response plan is critical. This is particularly true for health care providers and other HIPAA covered entities and business associates. The federal Office for Civil Rights has provided guidance for dealing with ransomware attacks. Notably, the guidance provides that when PHI (protected health information) is encrypted in such an attack, it is presumed to be a breach and notification required unless the entity determines the incident constitutes a low probability of compromise. The guidance adds that:

> Although entities are required to consider the four factors listed above in conducting their risk assessments to determine whether there is a low probability of compromise of the ePHI, entities are encouraged to consider additional factors, as needed, to appropriately evaluate the risk that the PHI has been compromised. If, for example, there is high risk of unavailability of the data, or high risk to the integrity of the data, such additional factors may indicate compromise. In those cases, entities must provide notification to individuals without unreasonable delay, particularly given that any delay may impact healthcare service and patient safety.

Taking steps to prevent an attack is important, but all SMEs, including those in the healthcare sector, also need to be prepared to respond to these and similar kinds of attacks. Failure to take these steps could have substantial effects on the business, including causing the business to close.