Published on *The National Law Review* https://natlawreview.com

A New Low For Hackers – Threatening to Disclose Patient Medical, Mental Health Records as Ransom for Payment

Article By:

Joseph J. Lazzarotti

Ransomware is a scary term for many business leaders and CISOs who dread being hit with a malware attack that locks up their data and could shut down operations. They expect to find that oddly-worded ransom note advising how they could recover access to their data, for a sizable fee of course. For a variety of reasons, including improved controls, backups, a loathe for paying criminal threat actors, organizations are increasingly refusing to pay hackers.

Hackers have responded to these refusals with threats to disclose sensitive personal information online and even resorting to directly contacting the individuals whose data has been compromised.

A Wall Street Journal article this morning speaks to this disturbing trend in data breaches. Vastaamo, a psychotherapy treatment center in Helsinki, was hit with a cyberattack in 2020. The hackers exfiltrated sensitive patient mental health records of 33,000 patients and threatened to disclose them online unless Vastaamo paid the ransom – approximately 400,000 euros.

According to the article:

> "When the clinic didn't pay, the hacker pressed individual patients for payment with bullying emails…one victim said the hacker gave her 24 hours to pay around 200 euros in bitcoin, or her therapy records would be posted."

Going directly to the affected individuals, whether they be patients, employees, students, etc. allows the hackers to also apply significant pressure on the organization to pay a much larger sum.

The decision to pay or not to pay a ransom comes with a range of critical considerations, some of which are discussed here. In the fog of an attack, with the press, government agencies, affiliates, and/or patients or other affected individuals looking to the organization for answers, working to develop an effective strategy is far more difficult. Increasing preparedness will not make this process easy, however, tough decisions need to be made. But working through these kinds of scenarios and planning generally for an attack will better equip executives and the board to work through the facts

of their case and make better decisions more quickly.

National Law Review, Volume XIII, Number 134