WSJ PRO

https://www.wsj.com/articles/rise-in-ransomware-brings-a-growing-role-for-negotiators-11571218201

Rise in Ransomware Brings a Growing Role for Negotiators

For companies that decide to pay, it's important to establish hackers can actually unlock files

The FBI has advised organizations not to pay ransoms in part because there is no guarantee hackers will restore data. PHOTO: CHIP SOMODEVILLA/GETTY IMAGES

By Adam Janofsky

Oct. 16, 2019 5:30 am ET | WSJ PRO

As ransomware spreads to hospitals and businesses across the country, victims are discovering that resolving these incidents is more complicated than deciding whether or not to pay up.

A key question is whether the attacker can actually unlock the encrypted data, said Robert Shimberg, an attorney at law firm Hill Ward Henderson PA. The Federal Bureau of Investigation warned companies this month of "high-impact ransomware attacks," advising organizations to avoid paying ransoms in part because there is no guarantee that data will be restored.

"You want to have as much assurance as possible that if you pay money to someone they can provide a deliverable to you—otherwise, you're just throwing money away," Mr. Shimberg said.

His firm negotiated with a hacker a few months ago on behalf of a client whose computer systems and backups were locked down. The attacker demanded a six-figure ransom.

> "Before we discussed payment, we told them you need to provide us with proof," Mr. Shimberg said.

His firm sent the hackers a few files that had been encrypted in the attack and they were able to unlock them. Negotiating also got the hackers to cut their price to "significantly less" than the original demand, said Mr. Shimberg. He declined to give more details.

Insurer Chubb Ltd. said its insurance claims show an 84% increase in ransomware attacks from 2017 to 2018, according to an analysis it published this month. In the first half of 2019, such claims outnumbered those for all of 2018, according to the report.

Todd Eppler, chief executive of DeSoto Regional Health System in western Louisiana, said his organization spent about $50,000 responding to a ransomware attack in 2017. He reported the incident to the FBI, which recommended that he not pay. He ultimately agreed because the attack affected only his organization's email server and didn't compromise medical records or other sensitive information.

"It still cost us a lot of money to take a server offline, bag it, tag it, never use it again and build a new server from backup," Mr. Eppler said.

Since then, DeSoto has spent an additional $20,000 to $30,000 a year on cybersecurity, including things like cyber insurance, consulting and security tools, he said.

Paying a ransom doesn't always make sense, Mr. Shimberg said. Victims must calculate the expense of a prolonged disruption and the price of rebuilding lost systems and data, and compare those to the amount demanded and how likely it is that the recovery will be successful, he said.

Organizations that do decide to negotiate should always involve law enforcement to leverage their expertise and help crack down on the schemes, he said. They should also consult with third-party IT experts to make sure that any decryption key or file sent by attackers won't cause additional damage.

In general, it doesn't hurt for organizations to try to broker a better deal with the attackers, he said. "The worst they can say is that this is not negotiable."

Write to Adam Janofsky at adam.janofsky@wsj.com