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

Ransomware—to Pay or Not to Pay and Should We Get a Bitcoin Wallet Just in Case?

Article By:

Linn F. Freedman

There's nothing worse than paying criminals. And paying a ransom for data is just that—paying criminals for a criminal act. All you get out of the payment is access to your data. It doesn't fix the vulnerability or the root problem. Let the record reflect that the FBI does not recommend paying ransoms to cybercriminals.

It is being reported that companies are paying ransom at a faster rate than ever before. Part of the reason for the payments is a response to the experiences of others, including the City of Baltimore, which expended far more resources in recovering from its ransomware attack than the amount requested by the criminals. However, if you look at what the City of Baltimore bought in response to the ransomware attack—although it was more than the ransom requested—it was an **investment** in its future security because it upgraded its systems and equipment to protect against future cyber-attacks. The investment was for the future—not a payment to line the criminals' pockets and leave the system in a state of vulnerability for another attack. When determining whether to pay a ransom, companies may wish to consider whether it is an extortion payment that only buys back access to their own data and doesn't fix the vulnerability, or an **investment in appropriate equipment and protection for the future**.

It used to be that companies would consider paying a ransom if they did not have appropriate data back-up systems to migrate to following a ransomware attack. Everyone now knows that the response to a ransomware incident is to have a robust and tested back-up system so you can shut off the infected system and get the company back up and running on the back-up if it was not also infected. Companies that did not have a back-up system had to consider whether or not to pay the ransom. Recently, companies with a back-up system have told attackers to go pound sand, migrated to the back-up system, and killed the old system.

Unfortunately, as companies implement more robust incident response plans, and are able to recover from ransomware attacks without paying ransom, cyber criminals are getting more sophisticated and figuring out how to stay ahead of that "go pound sand" response from victims. Recently, it has been reported that the cyber-criminal group MAZE is infecting businesses with ransomware and exfiltrating company data. Even if a company has sufficient back-ups, and may not need to pay for the decryption key, MAZE has exfiltrated sensitive company data and personal information, and requires

payment of a ransom for certification of destruction of the company data. If the company doesn't pay the ransom amount to be assured of that destruction, the attacker leaks the company data onto the web. MAZE actually hosts a website that lists all of its victims to try to shame them into paying the ransom. If the company pays the ransom, supposedly MAZE will abide by its word and not leak the data.

The consideration of whether or not to pay a ransom is very complicated and each scenario, risk analysis and business decision is different. The operative word is complicated. It is wise for companies to consider the risk of a ransomware attack like those MAZE employs and how it would respond if it were to become a victim of that type of ransomware attack. It is also wise for companies to determine whether they have insurance coverage for a ransom payment.

Some companies consider setting up a bitcoin wallet in the event they decide to pay a ransom following an attack. Paying a ransom to criminals has serious legal implications, which companies should explore carefully with their legal counsel. It is important to know what laws apply and to consider compliance with those laws before jumping into setting up accounts, negotiating directly with the criminals or paying a ransom. Remember that MAZE and other hacking groups are criminals and dealing with them directly is not just a business transaction.

National Law Review, Volume X, Number 44