GLOBAL DATA REVIEW

Credit: istock.com/urbazon

FBI softens line on ransomware payments

Robert Hart | **04 October 2019**

Observers say that the FBI is now recognising the “reality” that some ransomware victims will defy the agency’s recommendations and give in to hackers’ demands.

In guidance released this week, the FBI underlined that it still “does not advocate paying a ransom” when systems are infiltrated – but urged victims to get in touch “whether they have decided to pay the ransom or not”.

“Doing so provides investigators with the critical information they need to track ransomware attackers, hold them accountable under US law, and prevent future attacks,” it said.

The FBI had previously taken a hardline approach to ransomware demands, insisting that victims should not capitulate to hackers' demands.

Celeste Koeleveld, a partner at Clifford Chance in New York, told GDR that a section dedicated to answering whether victims should pay a ransom is a "subtle" acknowledgement on behalf of the agency that, despite its advice, people have been giving in to hackers' demands.

Aldo Leiva, of counsel at Baker Donelson Bearman in Fort Lauderdale, told GDR the updated guidance is "consistent with and reinforces" earlier guidance published by the agency. "It also provides additional examples of how payment of ransoms does not guarantee access to the victim's data".

The agency said some victims never receive decryption keys once they have paid a ransom and that flawed encryption algorithms, which hackers use to extort their victims, can leave data inaccessible even with a valid decryption key. It also said paying hackers' demands "emboldens" criminals by creating an "alluring and lucrative enterprise."

Luke Dembosky at Debevoise & Plimpton in Washington, DC said the guidelines were "carefully written to acknowledge that reality … the FBI recognises that ransomware victims sometimes don't have a real choice but to pay".

"The good news is that there is now a playbook of sorts forming up on how to prevent, detect, and minimise the impact of ransomware, as well as how to deal with the legal and practical issues," he said.

Walter Andrews, a partner at Hunton Andrews Kurth in Miami, told GDR that the guidelines show that the FBI "may be giving into the reality that … the payment of ransomware [ransoms] is now inevitable."

Andrews noted that the insurance industry's aggressive marketing of ransomware policies means "policyholders now have access to insurance money to pay cybercriminals who have engaged in ransomware attacks." It would be very hard for an insured organisation to not make the payment given the consequences, he said.

"The 'good' news is that the crooks understand that they have to actually [release] decryption keys or future ransomware attacks will not be successful because victims will not make payments that do not successfully stop the attacks."

Cybersecurity, Policy