KAUFMAN | DOLOWICH

Mansfield Rule Certified 2022-2023

Weighing Effects of Treasury's Ransomware Pay Warnings on Cyber Victims and Insurers, *Insurance Journal, ft. Eric Stern*

Eric B. Stern, partner and co-chair of the KD Data Privacy & Cybersecurity Practice Group, was quoted in an Insurance Journal article on the Treasury Department warning about paying ransomware demands written by Andrew Simpson.

Recent warnings from the U.S. Treasury about paying ransomware demands are unlikely to substantially change how cyber insurers cover or handle such situations, according to experts.

However, the advisories are likely to up the pressure on ransomware victims to make sure that they comply with all anti-money laundering and sanctions regulations.

The warnings came in advisories from a pair of Treasury agencies, one from the Financial Crimes Enforcement Network (FinCEN) and the other from the Office of Foreign Assets Control (OFAC).

The advisories have been issued at a time when experts report that ransomware attacks are rising and just weeks after leaked confidential Treasury filings indicate that money laundering and financing of terrorists as reported by major financial institutions remains a major problem.

FinCEN's advisory reminds businesses that any entity engaged in money services activities must register with FinCEN and must file suspicious activity reports (SARs) "if it knows, suspects, or has reason to suspect" that a transaction involves $5,000 or more in funds or other assets and involves funds derived from illegal activity.

Role of Insurance

Insurance is an important part of the process of recovering from ransomware attacks.

"Insurance coverage has grown to become a critical step for organizations in preparing for possible ransomware attacks," according to Eric Stern, partner and co-chair, Data Privacy & Cybersecurity Practice Group, at Kaufman Dolowich & Voluck, in New York.

He notes that coverage for ransomware attacks may fall under different policy lines, depending on the policy language, including cyber-coverage policies, which are the most common. Also depending on language, some policies insure against financial losses, as well as provide the aid of forensic and IT security response teams in managing an ongoing attack.

"This all-encompassing approach has led to insurers becoming a necessary part of an organization's response and recovery efforts," he said.

While insurers may offer advice, insureds are the ones who decide whether to pay a ransom in hopes the attacker will provide a decryption key or decide to refuse payment and suffer the losses that can be major. A ransom payment facilitator is often used. In these negotiations.

No Insurance Change

These experts do not anticipate insurers altering their role, coverages or services because of the advisories in any major way.

"Insurers will need to be cognizant of the potential penalties they may incur if they attempt to negotiate with ransomware hackers. Insurers should work to have controls in place to prevent prohibited payments and work with the insured and counsel in creating a response plan in light of the advisory," advised Stern.

Insurers might want to require their insureds to undergo preventative compliance training in an effort to mitigate any potential penalties they may face under the advisory. They should also be active in providing competent counsel as part of the response to ensure compliance with the advisory, Stern said.

Victim Burden

While there may be no big change for insurers, ransomware victims may wonder what to expect in terms of government enforcement of the rules discouraging ransomware payments.

Stern said that while potential liability has existed in the past for any party making payments to organizations designated as malicious actors, there has been no explicit guidance in the ransomware context in the past.

"Unfortunately, any non-government entity will struggle to ascertain the identity of a ransomware hacker – let alone to determine if they have been designated a malicious actor by OFAC. This advisory will add another step to an already complex and stressful time for ransomware victims. Also, considering that time is of the essence in ransomware situations, the added difficult step of identifying the malicious actor will create challenging decisions as insurers and response teams balance the threat of data loss with the threat of sanctions," he said.