Proskauer

Regulatory Crackdown on Ransomware

The Capital Commitment Blog on **December 14, 2020**

Ransomware is a Serious and Growing Problem

In recent years, Ransomware has evolved from merely encrypting files/disabling networks in solicitation of ransom, to sophisticated attacks that often involve actual data access, theft and sometimes, the threat of publication. These sophisticated malware attacks frequently destroy backups and provide criminals even more leverage over their victims, coercing them to pay ransoms. Ransomware does not just target businesses – it is often used to attack hospitals, research institutions, and other public services that are especially critical during this global pandemic.

It is increasingly common for Ransomware attacks to be associated with large sophisticated cyber-criminal organizations, with a central entity providing the tools, training, and ability to collect ransoms and sending its "associates" out to cause harm. As long as victims continue to pay ransoms, Ransomware is able to expand. Ransomware is also being adapted for new, criminal purposes. Increasingly, hackers associated with countries like Iran and North Korea are using Ransomware to generate an influx of cash into their economic streams and bypass economic sanctions. Faced with an urgent need to stop the spread of Ransomware, law enforcement is now moving past its old strategy of strongly discouraging victims from paying ransoms. Regulatory agencies – such as OFAC and the SEC – are implementing regulations to prevent victims from paying ransom to buy their way out of a Ransomware attack. These regulations arm law enforcement with a new enforcement mechanism – allowing them to punish companies who choose to pay ransom in the face of a Ransomware attack. Accordingly, they signal a new area of regulatory enforcement that will likely become the government's most powerful tool to curb the spread of Ransomware.

Regulatory Changes to Combat Ransomware

In the absence of evidence of data access or exfiltration, a Ransomware incident may not be considered a breach, and therefore, may fall outside any reporting requirements for cyber-incidents. Accordingly, in those circumstances, an organization could pay the ransom, potentially allowing it to restore functionality and avoid the reputational harm that would follow publication of a successful attack. But keeping these attacks in the dark creates a ripple effect in cybersecurity through which the criminal actors simply continue to perpetrate Ransomware attacks.

In October, OFAC issued an Advisory making clear that any payment made to a sanctioned entity – even where the payment is made under the duress of a Ransomware attack – would be a violation of federal sanctions regulations. Significantly, OFAC sanctions apply with strict liability, so the intent of the victim is no defense, nor is the victim's lack of knowledge that the payment is going to a sanctioned entity. In fact, the Advisory dispels any hope that OFAC might consider a victim's lack of knowledge and intent as a mitigating factor – as it occasionally does in other contexts. The Advisory makes crystal clear that OFAC intends to enforce these regulations aggressively, even where a victim did not know it was paying a sanctioned party: "OFAC may impose civil penalties for sanctions violations based on strict liability, meaning that a person subject to U.S. jurisdiction may be held civilly liable even if it did not know or have reason to know it was engaging in a transaction with a person that is prohibited under sanctions laws and regulations administered by OFAC." This raises a serious concern: in the context of Ransomware payments, where a criminal actor conceals its true identity, it could be difficult to determine exactly who will receive a ransom payment, and whether the party demanding payment is a sanctioned entity. Ransomware attackers also force victims to make ransom payments through non-bank methods, often specific cryptocurrencies like Monero, so one could not even rely on wire information or other ways to identify the recipient of a payment. Under these circumstances, it is nearly impossible for a victim to be completely sure that a ransom payment is not directed to a sanctioned entity.

An evolving Ransomware threat, coupled with OFAC's Advisory, will also likely increase the number of events that need to be disclosed under the SEC's latest cybersecurity guidance. The guidance describes disclosure requirements as they relate to Ransomware and other cyber-attacks. According to the guidance, companies are required to disclose material information in periodic reports, subject to Securities Act and Exchange Act obligations, and in certain instances, in current reports. Disclosure requirements are tied to materiality, which requires a company to disclose "such further material information, if any, as may be necessary to make the required statements, in light of the circumstances under which they are made, not misleading." The SEC will consider information to be material if there is a "substantial likelihood that a reasonable investor would consider the information important in making an investment decision or that disclosure of the omitted information would have been viewed by the reasonable investor as having significantly altered the total mix of information available." The regulatory risks of making any ransom payment, as well as the broader criminal goals of Ransomware attacks today, will likely mean that more attacks will need to be reported as material events.

Takeaways

OFAC's new Advisory on Ransomware raises important questions about OFAC's enforcement priorities as well as its compliance expectations. For example, the Advisory raises the question of whether one could ever conduct a transaction with a party that hasn't fully identified itself, and at the very least, suggests the need for heightened due diligence in these circumstances should an organization still choose to pay the ransom despite the legal risk. The Advisory also suggests that OFAC may take a more limited view of mitigating circumstances – such as lack of knowledge and duress — into account for sanctions violations in other contexts beyond Ransomware. One open issue is determining what kind of weight OFAC will give, if any, to a company's reliance on advice from an entirely different government agency – such as the FBI – about whether a payment was sanctions compliant.

While it may not be illegal per se to pay a ransom to a criminal that is not associated with a sanctioned entity, it is often impossible to determine who the criminal actors are behind the attack. Any entity considering paying a ransom, and the ecosystem that might support such a payment, should consider this risk as they evaluate the decision of whether or not to pay a ransom.

Firms should consider the impact of the OFAC requirements (and other regulations that will inevitably emerge to address Ransomware concerns) in their contracting with third parties, to ensure that their partners understand what will be expected of them in the event of a Ransomware incident. The goal of law enforcement appears to be that the combination of improved reporting plus disincentives for paying ransoms will disable, and eventually prevent, future threats of Ransomware.

View Original

Related Professionals

- **Seetha Ramachandran**
  Partner
- **Nolan M. Goldberg**
  Partner
- **Hena V. Balan**
  Associate