CYBER UPDATE

SCS AGENCY INSURANCE

Key Takeaways From OFAC's Ransomware Guidance

To address the epidemic of ransomware attacks against public and private entities, the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) updated its advisory on ransomware payments and included the first-ever sanctioning of virtual currency exchange. The Updated Advisory addresses the sanctions risks associated with paying ransomware actors. It also outlines OFAC's expectations that companies take meaningful steps to defend against and mitigate ransomware attacks, only paying a ransom as a last resort.

Since ransom payments to certain embargoed countries or threat actors may be unlawful, one of OFAC's primary purposes is to prevent companies from paying ransom in countries that the U.S. has sanctions against, such as Cuba, Iran, North Korea and Russia. In fact, OFAC has specifically sanctioned ransomware attackers and facilitators of ransomware transactions, including virtual currency exchanges. OFAC does not offer any exemptions for ransomware transactions involving sanctioned parties.

This article discusses the updated guidance, why it's important and steps organizations should take in the event of a ransomware attack.

Updated Guidance

OFAC first published a ransomware advisory on October 1, 2020, to explain the Treasury's views on potential sanctions risks involved in ransomware payments. While the Updated Advisory builds upon the Original Advisory, there are several key differences, including:

- **Explicitly stating that companies should not pay ransomware attackers**—The federal government has consistently discouraged organizations from paying ransomware attackers, but the Updated Advisory is the first time this stance is explicitly stated in clear terms.
- **Taking the victim company's prevention efforts into consideration**—Both advisories provide various recommendations for mitigating risks and penalties under OFAC rules; however, if it is ultimately determined the company violated sanctions, the Updated Advisory will consider a victim company's efforts in preventing attacks and minimizing harm. Any company that finds itself paying a ransom because it failed to adequately invest in cybersecurity could face harsh penalties from OFAC and other federal government agencies. All those involved in facilitating the payment—including financial institutions, insurers, incident response firms and extortion payment negotiators—could be held liable for criminal and civil penalties.
- **Self-reporting ransomware attacks and payment**—The Updated Advisory recommends that victims self-report incidents to the Cybersecurity and Infrastructure Security Agency, their local FBI field office, the

FBI Internet Crime Complaint Center, their local U.S. Secret Service Office and the Treasury's Office of Cybersecurity and Critical Infrastructure Protection.

The Importance of the Updated Advisory

The Updated Advisory addresses the nation's cybersecurity and underscores the seriousness of the threat posed by ransomware. In fact, there was a 225% increase in ransomware losses from 2019 to 2020, according to the FBI. The new guidance also incentivizes companies to prepare for attacks and cooperate fully with the government in the event of an attack. Organizations should consider the Updated Advisory when designing and implementing cybersecurity programs.

In the Event of a Ransomware Attack

Companies should take the necessary cybersecurity steps to prevent ransomware attacks from occurring. However, with the Updated Advisory in mind, organizations should take the following actions in the event of a ransomware attack:

- **Don't pay the ransom.** OFAC strongly discourages paying ransoms since payments may be sanctions violations and embolden bad actors—who often don't stick to their end of the bargain—to repeat their crimes and potentially threaten national security. To better avoid sanctions violations, don't pay the ransom and strengthen system defenses to prevent attacks from occurring in the first place.
- **Contact and cooperate with OFAC and other relevant government agencies.** Organizations should contact OFAC if there is any reason to suspect that a threat actor is sanctioned or connected to someone who is. OFAC may provide significant mitigation for voluntary self-disclosure of potential violations when determining the appropriate enforcement action.
- **Beware of crypto exchanges.** For the first time, OFAC designated property-blocking sanctions for virtual currency exchanges that facilitated ransomware transactions for ransomware actors. OFAC added SUEX OTC, S.R.O (SUEX OTC), a Russia-based cryptocurrency exchange, to its Specially Designated Nationals and Blocked Persons Lists. As a result of the designation, U.S. persons are prohibited from engaging in or facilitating virtually all transactions involving SUEX OTC.

Under the Updated Advisory, ransomware victims and those who assist them must remain attentive to U.S. sanctions compliance obligations. For more cybersecurity guidance, contact us today.