Ransomware Payments Sanctions Avoided with Risk-based Compliance Program

The U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) recently issued an advisory to highlight the sanctions risks of ransomware payments. The advisory warns companies and others that ransomware payments to cyber criminals on OFAC's blocked persons lists and those covered by embargoes are prohibited.

Violators of OFAC regulations face financial sanctions that may be reduced if they meet certain conditions. "Under the Enforcement Guidelines… the existence, nature, and adequacy of a sanctions compliance program is a factor that OFAC may consider when determining an appropriate enforcement response," the OFAC notice reads.

"Now more than ever, preventative and recovery controls are necessary," stated Carl Mazzanti, President and Co-founder, eMazzanti Technologies. "This can all be achieved with eMazzanti's e365 services to protect your business."

Significant portions of the Treasury Department's advisory are presented below to highlight the importance of appropriate ransomware preventative measures to mitigate the sanctions risk.

Treasury Department Ransomware Payments Advisory

"The U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) is issuing an advisory to alert companies that engage with victims of ransomware attacks of the potential sanctions risks for facilitating ransomware payments," the advisory reads.

According to the Treasury Department notice, Demand for ransomware payments has increased during the COVID-19 pandemic as cyber actors target online systems that U.S. persons rely on to continue conducting business.

"Companies that facilitate ransomware payments to cyber actors on behalf of victims, including financial institutions, cyber insurance firms, and companies involved in digital forensics and incident response, not only encourage future ransomware payment demands but also may risk violating OFAC regulations," states the advisory.

"In recent years, ransomware attacks have become more focused, sophisticated, costly, and numerous. According to the Federal Bureau of Investigation's 2018 and 2019 Internet Crime Reports, there was a 37 percent annual increase in reported ransomware cases and a 147 percent annual increase in associated losses from 2018 to 2019."

While ransomware attacks hit large corporations, many ransomware attacks also target small- and medium-sized businesses, local government agencies, hospitals, and school districts. These organizations may be more vulnerable because they may lack resources to invest in cyber protection.

Facilitating Ransomware Payments on Behalf of a Victim May Violate OFAC Regulations

According to the advisory, under the authority of the International Emergency Economic Powers Act (IEEPA) or the Trading with the Enemy Act (TWEA), U.S. persons are generally prohibited from engaging in transactions, directly or indirectly, with individuals or entities ("persons") on OFAC's Specially Designated Nationals and Blocked Persons List (SDN List). Payments to other blocked persons, and those covered by comprehensive country or region embargoes (e.g., Cuba, Iran, North Korea, and Syria) are also prohibited.

Risk-based Compliance Programs Encouraged

The OFAC encourages financial institutions and other companies to implement a risk-based compliance program to mitigate exposure to sanctions-related violations. This also applies to companies that engage with victims of ransomware attacks, such as those involved in providing cyber insurance, digital forensics and incident response, and financial services that may involve processing ransom payments (including depository institutions and money services businesses).

The notice encourages the sanctions compliance programs of these companies to account for the risk that a ransomware payment may involve an SDN or blocked person or an embargoed jurisdiction.

Other Mitigating Factors

Under the OFAC Enforcement Guidelines, authorities will consider a company's self-initiated, timely, and complete report of a ransomware attack to law enforcement to be a significant mitigating factor in determining appropriate enforcement. OFAC will also consider a company's full and timely cooperation with law enforcement both during and after a ransomware attack to be a significant mitigating factor when evaluating a possible enforcement outcome.

Ransomware Help from Security Experts

As organizations work to prevent ransomware, they must ensure early detection, respond to attacks and enlist the help of qualified security experts. eMazzanti helps business leaders implement comprehensive, ransomware protection and crisis control procedures if required. For organizations with limited IT resources, eMazzanti provides reliable managed IT security services to keep your valuable information safe.