MARSH JLT SPECIALTY

INSIGHTS | OCTOBER 2020

What OFAC's Ransomware Advisory Means for US Companies

Ransomware attacks and ransom demands continue to be a major concern for cyber insurers and insurance buyers alike. Attackers are using ransomware to target businesses of all sizes with greater frequency, and their attacks are growing more severe. Ransom demands of $1 million or more are now routine, and some demands have exceeded $10 million.

Ransomware payments — and their reimbursement under insurance policies — remain a controversial topic because of their potential for moral hazard and the possibility that such payments will fund international criminal, terrorist, and/or state-sponsored cyber actors.

OFAC Alert Highlights Sanction Risks

On October 1, 2020, the US Treasury Department's Office of Foreign Assets Control (OFAC) published an advisory that addresses this issue. OFAC's advisory reiterates the prohibition against US businesses and persons conducting business or paying funds to any person on the "Specially Designated Nationals and Blocked Persons" (SDN) list. US companies can be sanctioned for any violation of OFAC's rules, even if they do not personally execute a transaction or know that a payment is being made to a prohibited organization or person.

For several years, OFAC regulations have restricted the ability of ransomware victims to pay attackers on the SDN list, regardless of whether the attacker is believed to be sponsored by an OFAC-prohibited state — for example, Iran or North Korea — or designated by OFAC as a malicious cyber actor — for example, Evil Corp. The advisory highlights potential sanction risks in the payment of cyber extortion demands and encourages companies and their advisors to report cyber extortion attacks to law enforcement and to contact OFAC immediately if they believe a request for a ransomware payment may involve a prohibited organization or person. The advisory does not address the process or timing of responses by OFAC.

As OFAC makes clear, the recent advisory does not change any applicable laws, regulations, or guidance in relation to payments being made in connection with ransom demands. Instead, it serves as a reminder — to US companies, ransom payment facilitators, and cyber insurers — that a regulatory framework on ransomware already exists and applies in these circumstances.

Conducting OFAC Reviews

Ransom payments and related investigation and negotiations expenses remain covered losses under the cyber extortion component of most cyber insurance policies. While other coverage and public policy considerations may prohibit them, the payment of extortion demands by US companies and reimbursement by cyber insurers is not prohibited by OFAC, unless a payment is being made to an SDN. However, ransomware victims, ransom payment facilitators, cyber insurers, and participating financial institutions remain prohibited from doing business with any parties on the SDN list, including payment of a ransom.

To reduce their risk of an OFAC sanctions violation, businesses should confirm that an OFAC review — often performed by a ransom payment facilitator — is completed prior to paying any ransomware demands. As noted in the advisory, organizations should also consider notifying law enforcement prior to paying any ransom; this may be taken into account by the Treasury Department when considering subsequent enforcement action.

MARSH

A recent analysis by the law firm BakerHostetler offers more insight into the background and implications of OFAC's ransomware advisory.

Reassessing Ransom Incident Response Plans

The OFAC advisory makes it all the more important for businesses to have an OFAC compliance program in place that specifically addresses the possibility of a ransom demand during a cyber event.

More broadly, companies that are reassessing their ransomware response practices in light of OFAC's recent statement should take this opportunity to reevaluate all aspects of their cyber incident response program. Organizations should review their plans with all key stakeholders that will be engaged during or following a ransomware incident, including parties that specialize in ransomware response.

As they review these plans, companies should:

- Review the OFAC policies and procedures of all parties that may be involved in a payment to threat actors. Beyond ensuring their own compliance with OFAC policies, businesses should be mindful that their payment facilitators, cyber insurers, and participating financial institutions are also subject to OFAC regulations. At the time of an incident, ransom negotiators generally take the lead in this type of analysis and can supplement the OFAC SDN list with their own list of prohibited threat actors; although this step is not specifically required by OFAC, it can offer added protection. Organizations should also seek an OFAC certification from a ransom payment facilitator after any payment is made.
- Evaluate how all contractual arrangements with external parties on the incident response team address OFAC-related liabilities. Given the strict liability provisions included in OFAC regulations, representations of compliance with OFAC or indemnification/hold harmless provisions should be considered.
- Consider reassessing company policies regarding the payment of extortion demands generally, and cyber demands specifically. Extortion payments can shorten the duration of an event and reduce its impact, but should be weighed against other factors, including corporate codes of conduct, bylaws, and reputational risks.
- Ensure alignment of ransomware response plans with other critical incident response plans, including business continuity, disaster recovery, and crisis management plans, in order to streamline response in the event multiple response plans are triggered. This can help eliminate redundant or inefficient actions, improve coordination of effort, and reduce the chance for missteps. In their incident response plans, organizations should also consider the potential timing of securing any necessary OFAC clearance.

Mitigating Ransomware Risk

In addition to reviewing programs designed to ensure OFAC compliance, organizations should seek to minimize the risks of ransomware and, where possible, mitigate factors that increase the likelihood or necessity of a ransomware payment. Specifically, companies should:

- Review and consider strengthening backup data and data restoration plans. This can reduce the risk of material data loss and business interruption in the event data or systems are infected, and may be a factor in deciding whether to make an extortion payment.
- Reassess data retention and security practices to eliminate the risk of exfiltration of personally identifiable information. The threat of disclosure of sensitive information by bad actors is frequently a major factor when a company is deciding whether to make a ransom payment.
- Address remote desktop protocol (RDP) vulnerabilities, including closing any open RDP ports and moving any required RDP access behind a VPN.

Marsh Can Help

Your Marsh Cyber team is available to help you address the ever-changing and escalating risk of ransomware and associated cyber extortion. In addition to services included in your cyber insurance policy, your planning can include support from Marsh's Cyber Incident Management and Claims Advocacy teams. We can help clients prepare for, respond to, and recover from ransomware attacks, and can work with you to:

- Identify potential vulnerabilities in your incident response plans.
- Quantify the potential financial impact of a ransomware event.
- Build your pre-incident readiness and mid/post-incident response capabilities.
- Secure broad insurance coverage to maximize your recovery in the event of a loss.
- Identify and leverage services from leading incident response vendors.

For more information, contact your Marsh representative or send us an email at cyber.risk@marsh.com.