Guidepost

THE RANSOMWARE PAYMENT RISK

Deciding whether or not to pay off a criminal that has crippled your organization's operations with ransomware is a painful undertaking. It is a crucial decision that must be made at a time often described as "pure chaos." Management, attorneys, IT staff, incident response/digital forensics experts, the communications team, insurance companies and others all take part in addressing the crisis with an eye toward restoring operations to normal as quickly as possible. Time is of the essence. When technical recovery options have been exhausted, many organizations reluctantly elect to make the payment in order to recover vital information and restore services. The decision to pay off a criminal is never made lightly … and it is not without risk.

Risks facing ransomware victims are expanding. The trend is moving toward attacks that not only present a risk of not being able to recover all or some encrypted data after the ransom is paid, to attacks that include a "secondary extortion" component. In these attacks, not only are the organization's files encrypted, but sensitive, confidential information is exfiltrated from the organization's network, and the criminals threaten to release it in a public forum if a ransom is not paid. The techniques used by the attackers are increasing in sophistication and effectiveness, and that trend is expected to continue.

As distressing as this seems (and it is), it is important to remember that when making the Hobson's choice to pay the ransom to the extortionist, the victim may face even more peril, this time, at the hands of the United States government.

The October 1, 2020 Department of Treasury, Office of Foreign Asset Control ("OFAC") *Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments* warned that companies that make or facilitate ransomware payments to sanctioned persons or those located in comprehensively sanctioned jurisdictions risk violating OFAC regulations and related laws. Penalties are imposed on a strict liability basis and knowing violations can lead to criminal liability. The problem is exacerbated by the fact that the cyber extortionists conceal their identities, and a ransomware victim is usually provided with little more than an email address and a cryptocurrency wallet which tends to be of little use when checking against OFAC's Sanctions List.

With that as a backdrop, it may seem almost inevitable that a ransomware victim will face significant liability if a cryptocurrency payment is made to a party that turns out to be a sanctioned person or entity. The good news is there

are steps an organization can take to lessen any potential OFAC penalty. It all comes down to making, and demonstrating, a good faith effort to do the things all companies should be doing anyway.

OFAC maintains broad discretion to determine whether, and to what extent, it will penalize organizations making payments to ransomware extortionists, and has signaled that there are steps an organization can take to reduce the chances that OFAC will pursue an enforcement action.

OFAC looks at whether the company took its compliance obligation seriously, and acted in a responsible way before, during and after a ransomware attack that is later determined to have resulted in a payment being made to a sanctioned person or entity. To avoid liability, a company must be prepared to present a thorough and well-documented account of its investigation, compliance efforts and a summary of its initial disclosure to, and ongoing cooperation with law enforcement. Preparation is the key to doing this effectively.

Recommendation: Preparation

Regardless of potential OFAC liability, preventing or minimizing the effects of a ransomware attack is essential. This is best achieved through a cyber threat mitigation program, based on a recognized framework that includes appropriate controls, business continuity resiliency and periodic employee training. Preventing or recovering from a ransomware attack without having to pay the ransom is certainly the best approach. However, the increase in both the volume and sophistication of ransomware attacks requires companies to prepare for scenarios in which the preventative measures taken are ineffective and management decides that payment should be made.

Update Your Compliance Program

If your company has a sanctions compliance program in place, it would be advisable to update it to include a process for ransomware payments as a last resort. If your company does not have a compliance program in place, it is still advisable to include a process for ransomware payment in your company's overall cyber incident response plan.

Plan on a Thorough Investigation

As futile as it may seem given the absence of information provided by the extortionist, documenting a process that includes timely notification to law enforcement as well as all investigative steps taken, and evidence considered prior to making the payment should be considered.

In addition to outlining internal roles, responsibilities and pre-selected external service providers that will assist in such a crisis, your program should anticipate the collection of information that would be helpful to law enforcement and regulators including but not limited to:

- Relevant email addresses (with associated metadata including IP addresses and timestamps)
- Virtual currency wallet address(es)
- Information about the Indicators of Compromise ("IOCs") and the ransomware variants used (including hashes)

and other Tactics, Techniques and Procedures ("TTPs") used by the attackers
- Network activity logs (including logins) and conclusions reached regarding the methods of infiltration and propagation across the company network
- Mobile device information, if appropriate (including IMEI numbers)
- Copies of any suspicious electronic communications (including timestamps)
- If any identity information can be ascertained regarding the attacker, the results of a check against OFAC's Sanctions List and, if possible, a more detailed analysis of whether there is evidence of a sanctions nexus

Have Your Providers in Place

The information referred to above should be collected by digital forensics/incident response (DFIR) investigators or other qualified service providers and internal staff who are appropriately trained to collect such information. It is best to have contracts in place with any external providers before the event, and to have appropriate contact information available to the internal team.

Be Prepared to Work with Law Enforcement

Experienced attorneys should be involved from the outset of any ransomware crisis. To satisfy OFAC requirements that appropriate due diligence be undertaken before payment is made, all investigative efforts and findings need to be thoroughly documented and turned over to law enforcement. Particularly in those cases where sensitive corporate data is stolen, attorneys should assist with law enforcement outreach and liaison, since in addition to providing its initial findings, the company should also expect to provide additional findings from any continued investigation to law enforcement, OFAC and others as appropriate.

Train, Assess, Stay Up to Date

This plan, whether an addendum to an existing sanctions compliance program, or part of a cyber mitigation response plan, should be included in the company's training program, and should be reviewed (and a gap analysis performed) by the company's internal auditors or a third-party expert. Annual risk assessments and table-top training exercises should be performed that include new information about this rapidly evolving threat.

The threat of ransomware is real and growing. Thoughtful and thorough preparation can help minimize both the impact of the attack itself and reduce the likelihood of an OFAC sanctions enforcement action.

KENNETH MENDELSON CISSP, CIPP, CISA, PCIP

Senior Managing Director

Ken Mendelson has spent more than 30 years at the intersection of law, information technology and public policy. As a member of the National Security Practice, Ken manages governance, risk and compliance projects and investigations, and conducts monitorships

and third-party audits in connection with mitigation agreements enforced by the Committee on Foreign Investment in the United States (CFIUS). In addition, he assists established and emerging companies with implementing and maintaining cybersecurity and privacy programs by developing cybersecurity policies, procedures and guidelines, and conducting risk-based cybersecurity assessments.