THE ALS GROUP

OFAC Advisory Makes Paying Cyber Extortion Ransom Illegal

Ransomware continues to be a major issue for companies regardless of the size. It may be hard to believe, but the reason for this lies with the victims, because the quickest and most often used resolution to the attack is to pay the ransom. While paying the ransom, may resolve a problem for an organization, it encourages cyber criminals to continue the attacks.

To combat it, OFAC, the U.S. Department of the Treasury's Office of Foreign Assets Control, issued an Advisory in October 2020 stating that paying the ransom to a malicious actor in a ransomware event could land a company in hot water; and by hot water I mean OFAC may impose civil fines and sanction violations.

The thought is that the less payment a malicious actor receives, the quicker ransomware threats will diminish.

Here is the excerpt from the October 2020 Advisory that speaks about this; "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."

Of course, refusing to pay the ransom and involving law enforcement adds time to the interruption of business. Time that most, simply, cannot afford.

On September 21, 2021 OFAC issued a new Advisory that puts even more onus on the ransomware victims to not only report the incident to law enforcement, but to take "meaningful steps" to reduce the risk of extortion through improvement of cybersecurity practices. The Cybersecurity and Infrastructure Security Agency's ("CISA") September 2020 Ransomware Guide clarifies those practices. They include developing incident response plans, maintaining offline backups of data, and employing authentication protocols.

Of course, these are only a few of the cybersecurity practices that companies should be implementing. To learn more on the subject read our recent blog titled "Five Tips to Help Prevent Ransomware". Hopefully, your IT team has already implemented these fairly simple measures.

If you need more information on any of the topics covered in this blog, or need help with any cyber risk related issues please contact Jon Edwards, at 732.395.4281 or jedwards@thealsgroup.com.