OFAC sanctions necessitate improved cybersecurity preparedness and an experienced incident response team

James J. Giszczak, Dominic A. Paluzzi | Tuesday, September 28, 2021

As ransomware incidents skyrocket across the country, the U.S. government continues its efforts to combat cybercrime through all avenues. Most recently, sanctions were levied against a cryptocurrency exchange for facilitating illegal financial transactions to sanctioned entities. The recent sanctions indicate that, more than ever, organizations must take steps to both mitigate risk and properly handle cyber security incidents through an experienced response team when they occur.

On Sept. 21, 2021, the United States Department of the Treasury's Office of Foreign Assets Control (OFAC) released an updated advisory on potential sanctions risks for facilitating ransomware payments, including the first-ever sanctions against a cryptocurrency exchange, Suex.io.

In its announcement, the U.S. Department of the Treasury alleged that Suex facilitated transactions related to at least eight ransomware variants, and as much as 40% of Suex's transaction volume was linked to known malicious actors. As a result, OFAC has placed Suex on its sanctioned entity list, formally called the Specially Designated Nationals and Blocked Persons (SDN) List. The designation puts Suex in a category with suspected terrorists and narcotics traffickers and enforces economic sanctions wherein U.S. businesses and individuals are forbidden to do business with the exchange, or face a penalty of **fines or prison.**

While OFAC's sanctions are a first of their kind, they are unlikely to be their last. Critically, the designation

of an exchange as an SDN underscores the government's position: paying or merely facilitating a payment to an attacker on the SDN list is sufficient for the government to impose strong sanctions.

With the potential for such strong penalties, McDonald Hopkins strongly urges all organizations to take action. In its advisory, OFAC emphasizes the importance of companies taking proactive measures to lower the risk of a ransomware incident, and notes that these proactive steps would be considered "mitigating factors" in any related enforcement action. At a minimum, organizations in every sector and of every size, should take immediate steps to:

- **Maintain *offline off-site* backups of data**, which will increase your ability to restore data without the need to purchase a decryption key.
- **Develop and regularly test an incident response plan.** An evolving and regularly practiced plan will decrease operational downtime, increase the speed of notification to regulatory authorities and law enforcement, and anticipate operational, legal, and communication issues that arise during a ransomware attack. McDonald Hopkins can help your team draft and adopt an incident response plan, and provide tabletop exercises that will guide you through your plan.
- **Institute cybersecurity training**, which will decrease the likelihood of human errors that lead to ransomware attacks (e.g., clicking on malicious links in emails, poor password hygiene, or using non-sanctioned electronic devices and peer-to-peer networks).
- **Deploy and regularly update endpoint detection & response software**, that identifies cyber threats and intrusions in real time, allowing your team to immediately respond to an incident.
- **Apply appropriate data minimization, access controls, and adopt strong data destruction policies.** As ransomware attacks increasingly involve data exfiltration and the leakage of victim's data, ensure that your organization does not retain unnecessary and, for sensitive data that is retained, ensure that only appropriate individuals have access.
- **Adopt multifactor authentication protocols**, which can prevent a bad actor from accessing your network or account using only compromised credentials. Even complex passwords alone are routinely compromised.
- **In the event of an incident, immediately engage an experienced incident response team**, which can assist you with minimizing risks (including sanctions) to your organization and employees.
- **Work with counsel to report the incident to law enforcement.**

The Data Privacy and Cybersecurity team at McDonald Hopkins is available to assist with preparing your organization to be in the best defensible position against these attackers. This includes performing privacy risk assessment reviews, developing offline and offsite backup plans, developing incident response plans, instituting cybersecurity training, and collaborating with organizations to engage a Managed Service Provider to ensure that your organization is regularly updating antivirus and anti-malware software, and employing authentication protocols, among others. After helping thousands of organizations in virtually every sector over the last thirteen years, the McDonald Hopkins' team brings a vast history of experience to your organization.

James J. Giszczak

Dominic A. Paluzzi