The Dangerous Intersection Between

OFAC AND RANSOMWARE

Ransomware—that insidious menace threatening every entity no matter its size or industry—took several dark turns in 2021, all intended to magnify its impact. Attacks on major supply chain players reverberated throughout the economy, the continued rise in ransomware-as-a-service (RaaS) gave more criminals the ability to launch attacks and the growing prevalence of threats to expose an entity's sensitive information, on top of locking up its systems, doubled the trouble for attack victims.

In response, the federal government is waging an all-out offensive against ransomware, and it's using everything in its arsenal, including Office of Foreign Assets Control (OFAC) sanctions. This is creating a tricky minefield in which entities who pay a ransom or are involved in paying one could violate OFAC regulations resulting in a significant civil money penalty (CMP) on top of the reputational and financial fallout from the ransomware attack itself.

Considering that 2021 OFAC CMPs totaled $20.9 million, including six fines over $1 million, now is the time for organizations to redouble their OFAC compliance efforts. The same is true for their cybersecurity measures, as the Financial Crimes Enforcement Network (FinCEN) reported $590 million worth of ransomware-related suspicious activity in the first six months of 2021, well over the $416 million reported in all of 2020.

DECONSTRUCTING THE FEDERAL OFFENSIVE TO COMBAT RANSOMWARE

In the wake of 2020 in which cybercriminals took their ransomware efforts to new heights amid the COVID-19 pandemic, the Wall Street Journal reported that the Department of Justice (DOJ) created a task force to curtail ransomware cyberattacks. A key goal of the Ransomware and Digital Extortion Task Force is to target "the entire digital ecosystem that supports" such attacks.

Barely two weeks later on May 7, Colonial Pipeline became the latest victim of ransomware. This cyber incident, which was quickly followed by a ransomware attack on the major meat supplier JBS Foods, revealed exactly how vulnerable the U.S. economy and supply chain are to this growing threat and created new urgency for the DOJ task force.

By June, the DOJ issued updated guidance to federal prosecutors designed to "enhance and centralize" internal tracking and prosecutions related to ransomware. One month later, the U.S. government launched stopransomware.gov. This one-stop resource includes links to report a ransomware attack, a ransomware checklist and a ransomware guide.

Despite both Colonial Pipeline and JBS Foods paying ransoms to their attackers, the federal ransomware guide reiterates previous public statements from federal law enforcement that discourage victims from paying ransoms because it believes this solution only motivates cybercriminals to carry out more attacks. To underscore that point, the U.S. government put more teeth into its recommendation against paying ransoms with an updated OFAC Advisory published in September, which emphasized that paying a ransom—or facilitating the payment of one—increases the risk of sanctions violations.

By June, the DOJ issued updated guidance to federal prosecutors designed to "enhance and centralize" internal tracking and prosecutions related to ransomware. One month later, the U.S. government launched stopransomware.gov.

KEY HIGHLIGHTS OF THE OFAC ADVISORY

- OFAC specifically noted that financial institutions, cyber insurance firms and digital forensic companies could be at risk of sanctions violations when facilitating a ransom payment.
- OFAC has designated several known malicious cyber actors for sanctions, including the developers or sponsors of the Cryptolocker, SamSam, WannaCry 2.0 and Dridex ransomware.
- OFAC has also designated a virtual currency exchange known to facilitate ransomware payments.
- When determining OFAC sanctions violations, certain factors can mitigate the punishment:
  - A risk-based OFAC compliance program
  - Strong cybersecurity practices that reduce ransomware threats
  - Reporting the attack to law enforcement and cooperating with the same

A FinCEN Advisory followed in November, which was intended to assist financial institutions in detecting and reporting ransomware payments in order to hold attackers accountable and prevent the proceeds from being laundered through the U.S. financial system. This provided further proof of the U.S. government's attempt to root out ransomware.

MOUNTING A WORTHY DEFENSIVE STRATEGY

The federal government doesn't intend to wage this war on its own. It expects large and small businesses alike to mount their own defensive strategies, which clearly requires a two-sided approach.

An Effective OFAC Compliance Program

All U.S. businesses (and citizens) are prohibited from transacting with persons or entities designated on OFAC's Specially Designated Nationals (SDN) list or within jurisdictions designated under its sanctions programs. Financial institutions as defined by the USA PATRIOT Act face particular OFAC scrutiny. This includes traditional banks, casinos, importers and exporters, insurance companies, jewelry and precious gem dealers, money service businesses, non-profits and charities, real estate and construction firms, the travel and tourism industry, and vehicle dealers.

Financial institutions as defined by the USA PATRIOT Act face particular OFAC scrutiny. This includes traditional banks, casinos, importers and exporters, insurance companies, jewelry and precious gem dealers, money service businesses, non-profits and charities, real estate and construction firms, the travel and tourism industry, and vehicle dealers.

Financial institutions are not the only businesses that routinely face high-dollar CMPs for OFAC sanctions violations. In recent years, OFAC has dealt hefty fines to firms in many other industries, including energy and fossil-fuel, technology, fintech, electronic payments and trading, transportation and logistics, and those within the supply chain, such as retailers, distributors, suppliers and manufacturers.

In 2019, OFAC published its Framework for OFAC Compliance, which outlined the five components needed for an effective program:

1. **Management commitment:** Giving the program appropriate resources, authority and autonomy to maintain effective OFAC compliance.
2. **Risk assessment:** Evaluating the sanctions risks posed by an organization's customers, products, services, supply chain, intermediaries, counter-parties, transactions and geographic locations.
3. **Internal controls:** Documenting how the findings in the risk assessment will be addressed through written policies and procedures.
4. **Testing and auditing:** Conducting an independent review of the program by internal or external parties and using its results to strengthen the compliance program.
5. **Training:** Providing annual OFAC education to all employees.

When screening against watchlists and conducting appropriate due diligence to confirm or rule out potential matches, including those related to ransomware payments, there are several ways to streamline the process and reduce the risk of violations:

Using outsourced list updates provided by a third-party that monitors SDN list changes, including the addition of ransomware developers or related virtual currency exchanges.

Implementing a comprehensive screening solution that automates much of the process for you, including reports on positive matches and the reduction of false positives.

Choosing a screening solution that includes enhanced features, such as single SDN look-ups and batch file runs, search and report capabilities, complete Customer Data Management and integration with other systems.

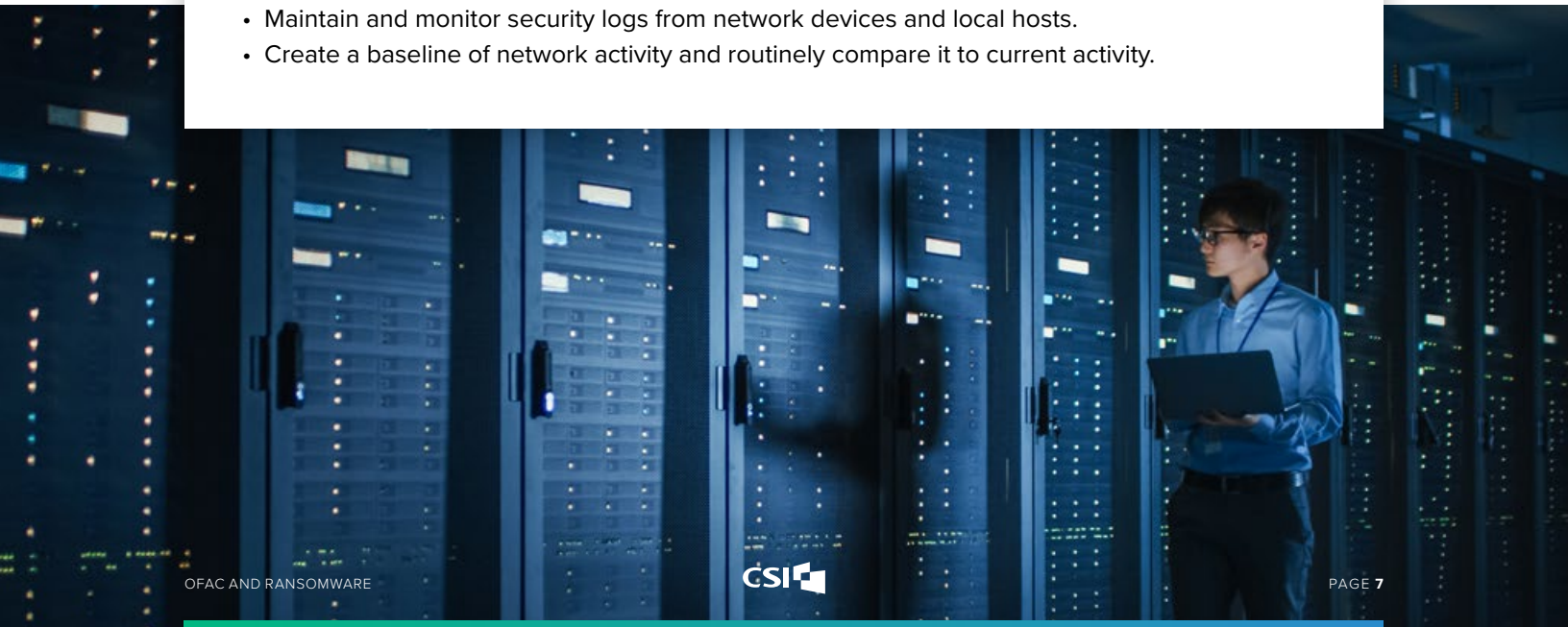
Looking for a screening solution with advanced word-matching techniques to cypher through the many initials, acronyms and name variations on the SDN list

A ROBUST CYBERSECURITY PROGRAM

As ransomware continues to pose a significant threat to organizations and cyber insurance becomes harder to get, there isn't a one-size-fits-all solution. At a minimum, it is essential to adequately protect sensitive files, which includes data-at-rest encryption, and limit access on a need-to-know basis through zero-trust architectures.

The 2020 Ransomware Guide, published by the Cybersecurity and Infrastructure Security Agency (CISA) and located on stopransomware.gov, provides an extensive list of best practices that make up a robust cybersecurity program to help prevent and mitigate ransomware attacks:

- Create and maintain offline, encrypted backups and regularly test them.
- Develop, maintain and test your cyber incident response plan, including notification procedures.
- Conduct vulnerability scanning and keep software and operating systems updated.
- Properly configure devices and enable security features.
- Follow best practices related to remote services.
- Don't allow outbound Server Message Block (SMB) protocol and remove outdated SMB.
- Train all users on the latest cybersecurity best practices and social engineering and ransomware trends and techniques.
- Employ filters at email gateways.
- Use Domain-based Message Authentication, Reporting and Conformance (DMARC) policy and verification.
- Disable Microsoft Office macro scripts for files being emailed.
- Keep antivirus and anti-malware software updated.
- Implement application directory allow listing on all assets.
- Explore the need for an intrusion detection system.
- Conduct adequate due diligence on all third-party and managed service providers.
- Use multi-factor authentication as much as possible.
- Limit privilege access as much as possible.
- Maintain and monitor a comprehensive inventory of hardware and software assets.
- Secure domain controllers.
- Maintain and monitor security logs from network devices and local hosts.
- Create a baseline of network activity and routinely compare it to current activity.



REMEMBER OFAC WHEN DEALING WITH A RANSOMWARE ATTACK

In today's environment, organizations must adopt best practices to prevent ransomware attacks, but they also need to be prepared to recover from one as the odds of being a victim grow every year. An inevitable aspect of recovery is deciding whether or not to pay the ransom to unlock your data and potentially prevent it from being publicly exposed. In making that decision, the possibility of violating OFAC sanctions must be factored into the equation. If it isn't, the OFAC fine could easily rival the amount of the ransom demand.

Furthermore, organizations in a position to help ransomware victims, such as financial institutions that might somehow facilitate the ransom payment, could also face a significant OFAC fine as a tangential participant in a ransomware incident.

From now on, OFAC violations and ransomware present an amalgamated threat to all U.S. businesses that must be recognized and addressed in order to limit its potential for grave financial harm.

ABOUT CSI

As a trusted partner in the regtech industry, CSI provides regulatory compliance software and services to thousands of customers worldwide, helping them stay compliant with today's top federal regulations, including OFAC, USA PATRIOT Act, GLBA and more. CSI's advanced compliance software solutions employ the latest technology to automate and streamline denied party screening, filing and fraud prevention to improve risk management and protect business integrity. As a compliance partner, CSI's innovative solutions help minimize false positives, reduce labor costs and strengthen practices in the face of rapid regulatory change. Visit www.csiweb.com for more information.

RESOURCES

[1] BSA/AML Program

[2] Legal Entity Beneficial Ownership

[3] Interagency Statement on Model Risk

[4] PwC's 2020 Global Economic Crime and Fraud Survey

[5] BSA/AML-Related Civil Money Penalties