COSMOS
Navigate the Compliance Universe

Report on Medicare Compliance Volume 30, Number 9. March 08, 2021
OFAC Fines Add to Ransomware Peril; 'It's a Between-a-Rock-and-a-Hard-Place Thing'

By Nina Youngstrom

Organizations have been warned by the U.S. Office of Foreign Assets Control (OFAC) that they may be fined if they pay ransom to "malicious cyber actors" to unlock their information systems. That complicates the decision whether to pay when attacked by ransomware and its variant, distributed denial of service (DDoS). Health systems should incorporate OFAC penalties into their prepayment due diligence and cybersecurity programs, attorneys said. They may pay the ransom anyway but will do it with their eyes open. This adds another dimension to ransomware at a time when the number of attacks is rising and cybercriminals may use artificial intelligence to make a bad situation worse.

In an Oct. 1 advisory,[1] OFAC stated that organizations are subject to fines if they paid ransom to people or entities on its "Specially Designated Nationals and Blocked Persons List (SDN List), other blocked persons, and those covered by comprehensive country or region embargoes (e.g., Cuba, the Crimea region of Ukraine, Iran, North Korea, and Syria)." That puts hospitals and health systems in a difficult position because they need to regain access to their protected health information (PHI) and business records immediately, especially if threat actors have hijacked their backup systems.

"It's a between-a-rock-and-a-hard-place thing," said Dave Summitt, chief information security officer at Moffitt Cancer Center in Tampa, Florida. "You may not have a choice to pay the ransom and make a recovery." But now hospitals must consider the risks in the advisory from OFAC, which is part of the Treasury Department, and "pull OFAC into their overall cyber preparedness and response plan," said David Rybicki, former deputy assistant attorney general. "Treasury wants to send a message you can face liability and will expect internal controls that are OFAC specific and pressure tested," said Rybicki, now an attorney with K&L Gates in Washington, D.C.

The OFAC advisory said there was a 37% increase in ransomware attacks from 2018 to 2019. "Our systems detect a ransomware attempt probably every week, three to four times," Summitt said. They're costing organizations a fortune, whether or not they pay the ransom. A cyberattack cost Universal Health Services, a huge hospital chain, $67 million in pre-tax losses, according to CyberScoop.[2] A Sept. 27 breach led to delayed billing, diversion of ambulances to competitors and spending on labor to restore connectivity.

The OFAC advisory said it could levy civil penalties on organizations for violations based on strict liability, which means they can be fined even if they didn't know they were engaging in a transaction with a person or entity on the SDN List.

'The Government Views You as the Perpetrator'

"You can have a situation where you are the victim and the government views you as the perpetrator," said attorney Christopher Swift, who investigated and prosecuted sanctions cases at the Treasury Department before he joined Foley & Lardner. In the eyes of OFAC, "it's kind of like paying a terrorist group." OFAC said it's

concerned that ransomware payments to cybercriminal organizations, such as Russia-based Evil Corp, "could be used to fund activities adverse to the national security and foreign policy objectives of the United States."

Organizations invite sanctions when they rush to pay ransom without investigating the hacker. "There is a knee-jerk reaction to 'get my stuff back as soon as possible because of HIPAA,' and that can sometimes lead people to make decisions before they know what they're dealing with," Swift said. "Make sure senior leaders know about the sanctions risk. When you have tabletop exercises or standard operating procedures to deal with ransomware, a sanctions assessment should be baked into that cake."

Whether to pay a ransom is always a torturous question. Hospitals don't want to encourage cybercriminals, and there's a risk they won't get the decryption key even if they pay. Sometimes hospitals say no and just rely on their backup systems, although the cybercriminals could post the PHI on the internet in retaliation. Whatever the calculation, the potential OFAC sanctions take hospitals into dangerous territory.

"It's important to recognize that the OFAC guidance doesn't stand for the proposition that some have attributed, which is you can never pay ransom payments," said former federal prosecutor Robert Trusiak, an attorney in Buffalo, New York. "You can in certain circumstances. But you need to appreciate, despite the fact that everyone is running around with their hair on fire because you don't have access and the threat actor is threatening to publish your PHI in 96 hours if you don't pay, that you need to do work items as it relates to ensuring you're not dealing with a terrorist organization."

That's where a forensic investigation comes in, Swift said. That will help hospitals figure out if the threat actor is a sanctioned entity. There are clues, such as the cryptocurrency wallet address, the type of malware used and whether the ransom demand suggests English is not the threat actor's first language. "All of these things go into the analysis of what flavor risk you have," he said.

HIPAA and OFAC: Carrot and the Stick

Whether hospitals pay the ransom depends on several factors, Rybicki said. They include the nature of the breach, patient and financial considerations, whether information was backed up, and whether the cybercriminal is on the SDN List. "There are a lot of covered entities that make the calculation they need to pay based on the gravity of the situation," Rybicki said. "But management would need to undertake a highly fact-specific analysis before acting."

The OFAC part is a prepayment due diligence matter for hospitals and other organizations, he said. "They need to determine using outside counsel and third-party vendors whether paying the ransom creates exposure," Rybicki said. OFAC will take into consideration the due diligence and internal controls if an organization unwittingly makes a ransomware payment to an entity on the SDN List.

Summitt is skeptical that the Treasury Department will fine a health care organization for paying ransom in the service of patients, and some of the attorneys agreed the OFAC advisory may be intended to motivate more effective cybersecurity programs. Trusiak thinks the federal government and New York state's Department of Financial Services, which on Feb. 4 published an OFAC-like framework,[3] are pursuing a carrot-and-stick approach to better cybersecurity, Trusiak said. The carrot is the HIPAA safe harbor enacted by Congress late last year in an amendment to the Health Information Technology for Economic and Clinical Health Act,[4] which was signed into law Jan. 5. It requires the HHS Office for Civil Rights to consider recognized security practices of covered entities when calculating fines for violations of HIPAA privacy and security rules. Penalties may be reduced if security practices have been in place for the previous 12 months. The provision is retroactive to Dec. 13, 2016, the signing of the 21st Century Cures Act.

The stick is the OFAC penalties. "Cybersecurity and ransom payments are quickly devolving into a Hobson's choice for providers," Trusiak said. You either pay the ransom and "risk being victimized twice, by the state or federal government or both, or don't pay and risk having your doors shuttered." He thinks implementing a zero-trust solution avoids the Hobson's choice. Zero trust, as the name implies, prevents people, internally and externally, from connecting to the network unless they have specifically been given permission through authentication. "A zero-trust solution right now is the best approach to hardening the cybersecurity environment," Trusiak said.

Sometimes You Can Just Say No

Sometimes ransomware attacks pose little threat and health care entities don't have to make risk calculations about OFAC, said Gina Bertolini, an attorney with K&L Gates in Research Triangle Park, North Carolina. She recently helped a provider in this position after an employee clicked on a phishing email from a hacker posing as a DHL carrier with a shipping update. The hackers unleashed malware, which remained in the provider's computer system undetected for months. The hackers were able to tap into and exfiltrate data, but it wasn't extensive enough to disrupt the provider's business, Bertolini said. Eventually, some employees noticed unusual activity and reported it. Although it took some time for the provider to find the ransom note, it didn't pay the threat actor, she said. After a forensic analysis, the provider determined the threat actor hadn't permanently removed anything, Bertolini said. "We had backups of everything," she noted. "Most of the records they accessed were business records." Because a small percent had PHI, the provider reported the breach to the HHS Office for Civil Rights and to patients. "They did everything right once they discovered it," she noted, including improving education and upgrading information technology tools.

Bertolini suggested health systems build ransomware protections and the OFAC due diligence process into their enterprise-wide HIPAA privacy and security program. "HIPAA has standards and specifications with built-in flexibilities for covered entities to determine for themselves how to protect the integrity of their PHI," she said. They should use that flexibility to determine what tools they need to prevent attacks and how to proceed if they have one. "A robust security compliance program integrates the OFAC guidance on ransomware," she noted.

Bad Actors Demand Ransom to Stop DDoS

There's more than one kind of ransomware attack; DDoS is another threat in this vein, Summitt said. Threat actors set up robocalls at such a high volume they jam phone lines, preventing people at hospitals from calling out and vice versa, which only stop when hospitals pays a ransom or when they take extra steps working with their telecom company, he said. Moffitt works closely with its telecom company to help prevent these events and has reported some to the FBI.

Hackers also have been calling physicians and other clinicians, pretending to be from the Department of Justice or state of Florida medical or pharmacy licensing agency. They tried to elicit personal information from some clinicians. "Sometimes it was to do prescription fraud," Summitt said. "It was really scary for the providers." They have been educated to contact Moffitt's cyber team when they receive these calls. "The overwhelming majority of the time, you hang up on the caller."

What lies ahead sends shivers down the spine. "Machine learning and artificial intelligence are starting to take off, and the bad actors are starting to take advantage of it," Summitt said. For example, they potentially can use deep fake video and audio to mimic the CEO and request a wire transfer or sensitive business/patient information. That's harder to prevent or expose than business email compromise, where hackers pose in email as CEOs or other executives.

To prevent ransomware attacks, Moffitt uses a "defense in depth" strategy. It starts with user education (e.g., on

phishing) because 65% to 95% of ransomware attacks occur through an email. Also, "we isolate all attachments and have them checked before we release them to users" and check incoming links. Another layer is workstation protection. "If [users] download a malicious user file, we don't allow it to propagate," Summitt said. Moffitt also does a lot of monitoring. If something is triggered, hopefully Moffitt's response is quick enough to remove the malware before it moves from computer to computer. "You don't rely on one control," he explained. "We probably have four layers of defense at Moffitt before a ransomware event can take hold." Other layers include the firewall, anti-virus software and patching. "There is no single bullet in defending against ransomware" because "it's high risk, high probability," Summitt said.

Attorney Jennifer Urban, with Foley & Lardner in Chicago, encourages organizations to work with the FBI and other law enforcement agencies when they're hit with ransomware attacks. Even organizations with the best cybersecurity will be victims of cybercrime.

"There's no foolproof security solution," Urban said. Organizations should focus on a risk-based method, she said. "You do your due diligence on the front end" and mitigate on the back end with security controls.

Contact Summit at dave.summitt@moffitt.org, Bertolini at gina.bertolini@klgates.com, Rybicki at david.rybicki@klgates.com, Trusiak at robert@trusiaklaw.com, Swift at cswift@foley.com and Urban at jurban@foley.com.

1 U.S. Department of the Treasury, "Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments," advisory, October 1, 2020, https://bit.ly/3kL666e.
2 Sean Lyngaas, "Universal Health Services reports $67 million in losses after apparent ransomware attack," CyberScoop, March 1, 2021, http://bit.ly/3s0odZ4.
3 New York state Department of Financial Services, "Cyber Insurance Risk Framework," Insurance Circular Letter No. 2, 23 NYCRR 500, February 4, 2021, http://on.ny.gov/3e9lvfG.
4 To amend the Health Information Technology for Economic and Clinical Health Act to require the Secretary of Health and Human Services to consider certain recognized security practices of covered entities and business associates when making certain determinations, and for other purposes, H.R. 7898, 116 Cong. (2020), http://bit.ly/2Lm9KG1.