Paying a hacking ransom could bring trouble; take steps to stay safe

by: Roy Edroso

Effective Oct 28, 2021
Published Nov 1, 2021
Last Reviewed Oct 28, 2021

PBN Perspectives

Can you get in trouble for paying off a ransomware crook? It's not out of the question, but you can reduce your chances if you follow a sound protocol before attempting to pay. Also be sure to emplace necessary safeguards before you get attacked.

Ransomware has become a massive problem for health care entities of every size and type (*PBN 4/26/21*). The urgency of unlocking the files that hackers lock up in a ransomware attack typically leads practices to pay the ransom rather than wait, fruitlessly, for law enforcement to find the culprit.
U.S. law enforcement agencies generally advise that you not pay the ransom. The FBI "does not support paying a ransom in response to a ransomware attack," the agency says at its "Scams and Safety: Ransomware" website.

At the same time, however, the FBI acknowledges the reality on the ground: While insisting that "paying ransoms emboldens criminals to target other organizations and provides an alluring and lucrative enterprise to other criminals," according to an Oct. 2, 2019 alert, the agency "understands that when businesses are faced with an inability to function, executives will evaluate all options to protect their shareholders, employees and customers."

The suggestion of flexibility may be going away, though. A May attack on the Colonial Pipeline that briefly interrupted oil and gas deliveries stirred fresh concerns that malign foreign actors could use ransomware tools to attack data, not merely for profit, but also for terrorism. On Oct. 1, The U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) reminded potential ransomware targets that, if their payoffs wound up going to any sanctioned entities on their interational list, paying a ransom could lead to penalties.

OFAC also warned it "may impose civil penalties for sanctions violations based on strict liability" in such cases, under the Economic Sanctions Enforcement Guidelines of federal law, which stipulated monetary penalties running into the hundreds of thousands of dollars. OFAC "encourages" ransomware victims to contact them, as well as other government agencies including the FBI, when they are attacked (*see resources, below*).

Check and call
Does that mean you could go up on federal charges if you pay ransomware perpetrators and they turn out to be terrorists? It's unlikely, but it does suggest some caution — and steps to take — when you find yourself facing a ransom demand.

First, OFAC has a web tool for searching their Sanctions Search List of prohibited entities (*see resources, below*). Experts tell *Part B News* that checking the list is one of the key good-faith gestures you should make to show that you're cooperating.

Richard Shenis, a partner with Hall Booth Smith in Charlotte, N.C., and leader of the firm's data privacy and cyber security practice says in these cases "we get the team of vendors that we work with — including forensic IT teams and vendors that specialize in communications and negotiations with the threat actor — to provide the client and myself a letter stating that they have checked the OFAC search list and we're good to go."

Theodore J. Kobus III, a partner with BakerHostetler in New York City and chair of the firm's digital assets and data management group, describes a typical collaboration: "The payment facilitator is going to do a compliance check that includes a review of the Bitcoin wallet and malware variant using a software program to determine whether the threat actor is attached to or associated with a [listed] group that is not necessarily immediately identified with this particular malware."

Meanwhile the lawyers "are using their connections with law enforcement, particularly the FBI, as well as information learned on other client engagements to determine the potential association of the threat actor," Kobus adds. "And of course, the digital forensics investigator is looking at the malware binary and other information gained through threat information sharing efforts with law enforcement and others. There may be different approaches, but all of these steps combined can give the client assurances that they're acting appropriately."

Whether or not you and your team find a listed actor, contact OFAC, suggests Joel B. Bruckman, an attorney with Freeborn & Peters in Chicago. "OFAC's recent guidance states that in the event that you 'suspect' that an entity or group demanding ransom may be on the sanctions list you are to promptly notify OFAC of the incident," he says.

Pay anyway?

What if you find your cyber-assailant is listed, but you decide that you need to pay up anyway because the threat to patient care is too urgent to ignore? OFAC has a "licensing" arrangement, applications for which it says it will review "on a case-by-case basis with a presumption of denial."

As a health care provider, you could "go to OFAC and apply for a license and stress that if a license is not granted, a loss of lives will occur or has occurred," Kobus says. "That may or may not take some time, unfortunately, or even not occur at all. But I would be hopeful that in special circumstances OFAC would act swiftly."

Time considerations may push you to pay in the absence of OFAC clearance. Would that situation mitigate OFAC's response? "That would vary on a case-by-case basis," Bruckman relays.

Whether your action is reasonable under the circumstances would be a factor. "For example, say you have offline backups of needed data," Bruckman says. "I'm mentioning this because it plays into whether the response you're proposing is reasonable. If you have the data and nonetheless choose to pay the ransom, it's fundamentally different than somebody who doesn't have accessible backups."

Your size and scope may come into play as well. "The threat exists, but the likelihood of [penalties] being imposed on a smaller health care organization, where they're already suffering because of having to pay the ransom and the impact on operations — that would to some degree seem like piling on," says Matt Fisher, general counsel for Carium, a virtual care platform, based in Worcester, Mass. "But if you're looking at a bigger organization where there might be more financial resources, maybe that becomes more attractive [to prosecutors]."

Further legal issues

Even if you take care of your OFAC obligations, you may not be out of the woods. Bruckman points out that federal agencies talk to one another and, if the attack suggests your defense of your data does not meet HIPAA requirements, HHS' Office for Civil Rights, which has ruled that ransomware attacks are reportable breaches, may bring action.

"I would say that most regulators are concerned about the security posture maturity of the company that experienced the attack," Kobus says. "If the client has robust security and the perpetrators were still able to get in, that's one thing; if the client doesn't have good security, that's something else."

Resources

FBI, "Scams and Safety: Ransomware": *www.fbi.gov/scams-and-safety/common-scams-and-crimes/ransomware*
FBO, "High-Impact Ransomware Attacks Threaten U.S. Businesses And Organizations," Oct. 2, 2019: *www.ic3.gov/Media/Y2019/PSA191002*
DOJ, Office of the Deputy Attorney General, "Guidance Regarding Investigations and Cases Related to Ransomware and Digital Extortion": *www.justice.gov/dag/page/file/1401231/download*
U.S. Treasury Department, "Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments," Oct. 1, 2021: *https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf*Office of Foreign Assets Control (OFAC) Sanctions Search List: *https://sanctionssearch.ofac.treas.gov/Details.aspx?id=26664*

BACK TO TOP