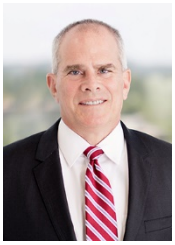
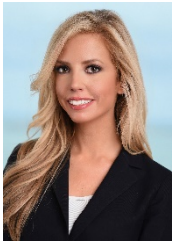
HUNTON ANDREWS KURTH

Lawyer Insights

OFAC Cyber Ransom Guidance Has Insurance Implications

By Walter Andrews, Andrea DeField and William Sowers
Published in Law360 | November 16, 2020

The U.S. Department of the Treasury's Office of Foreign Assets Control issued an advisory in early October reiterating that it considers the payment of ransom to certain cyber actors to be a violation of law, exposing the payer to civil penalties.[1]

That advisory, which OFAC expressly states applies to cyberinsurance companies, digital forensic and incident response companies, and financial services companies that process ransom payments, is likely to lead to cyberinsurers delaying their coverage determinations until such time as they may adequately investigate whether the threat actor is on an OFAC sanctions list and whether the ransom payment may violate the International Emergency Economic Powers Act or the Trading with the Enemy Act.

This may leave policyholders in a bind during the crucial minutes and hours after discovery of a ransomware attack: Do policyholders pay the ransom and risk no insurance coverage for that payment or, do policyholders refuse to pay the ransom and attempt to restore the encrypted data, despite what could be a lengthy interruption to their business operations or significant costs in restoring or recreating data?

While that decision should be made on a case-by-case basis under the advice of breach response counsel and law enforcement, fortunately, there are steps policyholders can take now to shore up their cyberinsurance coverage to ensure the broadest possible coverage for restoration and repair costs when a ransom is not paid.

What are ransomware attacks?

Ransomware attacks are cyberattacks in which, generally, a threat actor (1) demands a ransom in exchange for not encrypting data, not destroying data, or not blocking access to a computer system or data; or (2) demands a ransom in exchange for restoring access to a computer system or to unencrypt data that it has already encrypted.

The decision to pay is a financial one; the cost to pay a ransom is sometimes less expensive than a company's lost business income when its business operations or supply chain is interrupted, either partially or wholly, as a result of the attack.

Just this year, an Alabama city paid a $291,000 ransom to release its data,[2] and Oregon's Tillamook County paid a $300,000 ransom to release its data,[3] and defense contractor Communications & Power Industries paid $500,000 to release its data.[4] But ransom demands can be significantly higher.

In October, Software AG faced a $20 million ransom demand in order to decrypt the company's internal network.[5] When the company failed to pay, the threat actors published screenshots of company data on

the dark web, including employee passport and identification information.

The payment of ransoms had made ransomware a lucrative business for cybercriminal organizations. In fact, from the first quarter of 2020 to the second quarter of 2020, the average ransom payment increased 60%.[6]

Paying the ransom does not always mean that all systems and data will be fully restored. For instance, in the case of Communications & Power Industries, a threat actor accessed the company's computer system through a phishing attack — the threat actor sent an email with a malicious link that someone inside the company clicked, granting the threat actor access to the system.

The company paid the half-million dollar ransom, but a month and a half after the attack, still only one quarter of the company's computers were back online. That downtime can be very costly for businesses.

Not all companies choose to respond to ransomware attacks by paying the ransom. For example, in March, a fintech company, Finastra, was the victim of a ransomware attack.[7] But it did not pay the ransom; instead it shut down all of the thousands of infected or potentially infected servers. Because Finastra acted early, it was able to isolate infected servers and bring key services back online within days; however, its business income losses are unknown.

All of these costs and business losses can be covered by insurance. That insurance, though, may be impacted by the new OFAC advisory.

What is impact of the Office of Foreign Asset Control's new advisory?

The OFAC October advisory indicates that it is planning to use existing law to pursue civil penalties against organizations that pay ransom to persons on OFAC's specially designated nationals and blocked persons list, other blocked persons, and those covered by comprehensive country or regime embargoes (such as Cuba, the Crimea region of Ukraine, Iran, North Korea and Syria), as well as against those who assist organizations in making such payments, such as cyberinsurers.[8]

Further, the advisory warns that the liability will be strict liability, meaning that an organization can be liable for civil penalties even if it did not know or have reason to know that it was engaging in a transaction with a malicious cyber actor. Accordingly, the advisory recommends that such organizations implement "risk-based compliance program[s] to mitigate exposure to sanctions-related violations."

While the advisory does not create new law, it serves as a cautionary reminder of existing law that requires insurers to first make sure the threat actor is not on a prohibited persons list before paying a ransom.

However, it can be incredibly difficult to determine who is behind a ransomware attack, and every hour of delay to determine whether a threat actor has been designated as a malicious cyber actor can cost the victim thousands of dollars and reduce the likelihood that it can recover the ransomed information.

If the insurer cannot promptly determine whether the threat actor is a prohibited person, then the insurer may decide not to reimburse the victim out of fear that, if it does pay and the threat actor is later determined by law enforcement to be on OFAC's restricted list, it may face civil penalties.

OFAC Cyber Ransom Guidance Has Insurance Implications
By Walter Andrews, Andrea DeField and William Sowers
Law360 | November 16, 2020

As a result, insurers may consider including new exclusions or broadening existing exclusions in cyberinsurance policies so that coverage does not apply to ransomware attacks carried out by — or suspected to have been carried out by — designated prohibited cyber actors.

Further, even before the new exclusions go into effect, some insurers, when faced with a ransomware claim, may reserve rights and instruct the insured to act as a reasonably prudent uninsured organization would because the insurer cannot yet confirm or deny coverage.

That situation would leave the insured in a precarious position, where it must decide whether to pay a ransom, and risk the ransom being uninsured, or not pay the ransom, and risk significant business interruption losses and other investigation and restoration costs while trying to restore data from backups.

Ensure robust insurance coverage now to prevent denials later.

Fortunately, multiple types of insurance may provide some coverage for losses arising out of a ransomware attack.

First, a company's cyberinsurance policy usually includes express cyber extortion and/or ransomware coverage, which should cover the ransom, ransom negotiation costs, legal fees and forensic investigation.

Note that coverage for the ransom itself is usually a reimbursement coverage, so the insured pays the ransom and then the insurer reimburses the cost, if it finds that there is coverage under the policy. The uncertainty created by this delay in obtaining a coverage position from the insurer, however, may prove too risky for some corporate policyholders.

Thus, policyholders must ensure that they have at least the following coverages in place should they decide to not pay the ransom.[9]

- Robust cyber incident response and investigation coverage to cover costs associated with the forensic investigation of the cause, source and extent of the incident; costs to secure the network and terminate the attack; costs of legal advice on whether any public or regulatory notice is required; notice costs, if applicable; and public relations costs;

- Broad coverage for data restoration and recovery costs and digital asset loss, including coverage for bricking — when a piece of physical equipment is damaged or rendered useless due to malware — and betterment expenses to replace and/or upgrade or improve the computer system to eliminate vulnerabilities;

- Business interruption coverage to cover business income loss and extra expense, including forensic accounting resources and/or coverage for costs incurred to present a business interruption claim, as well as an extended period of indemnity to cover ramp-up costs after access to the network is restored to normal operating levels;

- Coverage for losses due to reputational harm as a result of the ransomware attack; and
- Liability coverages that cover defense costs incurred in responding to both claims and regulatory investigations that may arise following a ransomware attack, as well as for fines, penalties, and damages.

In addition to cyber policies, the following policies may also provide coverage.

A property insurance policy may include some coverage for restoration of systems and business interruption costs, usually called computer virus or computer hacking coverage. This coverage is usually subject to a sublimit.

Kidnap, ransom and extortion insurance is likely to provide cyber extortion coverage, including coverage for ransom payments. However, such coverage may be sublimited, and insurers may expressly limit coverage for remediation or investigation costs to ransom negotiation, advice on the ransom, and the ransom itself.

These policies may or may not also include business interruption coverage, which is usually purchased as an endorsement to the policy for a specified sublimit.

Some directors and officers policies may provide express coverage for liability arising out of a cyber or ransomware event by endorsement, but it is usually limited in amount and applies excess of any cyberinsurance policy. Any express coverage grant would need to be negotiated, particularly because some D&O policies now contain cyber exclusions.

Without such an endorsement, D&O policies may be limited in application to certain covered claims that arise out of the ransomware incident, such as a securities claim resulting from same.

What should policyholders do?

While policyholders and their insurers may be unsure as to whether paying a ransom will implicate OFAC's rules, subjecting them to OFAC civil penalties, with proactive insurance planning and risk management, policyholders should be able to ensure that their insurance coverage will nonetheless respond to the range of costs and losses that the policyholder faces should it decline to pay the ransom

Notes

1. U.S. Treasury Office of Foreign Assets Control, Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments (Oct. 1, 2020), https://home.treasury.gov/policy-issues/financial-sanctions/recent-actions/20201001.

2. Sarah Coble, Alabama City to Pay Cyber-Ransom, infosecurity Magazine (June 10, 2020), https://www.infosecurity-magazine.com/news/alabama-city-to-pay-cyberransom/#:~:text=Florence%20became%20a%20victim%20of,city%20didn't%20pay%20up (last visited Nov. 9, 2020).

3. Cody Mann, County Pays $300,000 for Cyberattack Ransom, Tillamook Headlight Herald (March 24, 2020), https://www.tillamookheadlightherald.com/news/county-pays-300-000-for-cyberattack-ransom/article_83e8ede2-63be-11ea-8323-ab4eb2deccd9.html.

4. Zack Whittaker, Defense Contractor CPI Knocked Offline by Ransomware Attack, Tech Crunch (March 5, 2020), https://techcrunch.com/2020/03/05/cpi-ransomware-defense-contractor/.

5. Catalin Cimpanu, German Tech Giant Software AG Down After Ransomware Attack, ZDNet (Oct. 9, 2020), https://www.zdnet.com/article/german-tech-giant-software-ag-down-after-ransomware-attack/.

6. Ransomware Attacks Fracture Between Enterprise and Ransomware-as-a-Service in Q2 as Demands Increase, Coverware (Aug. 3, 2020), https://www.coveware.com/blog/q2-2020-ransomware-marketplace-report.

7. Jordan Robertson, How Finastra Survived a Ransomware Attack Without Paying Ransom, Bloomberg Businessweek (April 7, 2020), https://www.google.com/search?q=finestra+ransomware&rlz=1C1GCEB_enUS918US919&oq=finestra+ransomware&aqs=chrome..69i57j0i13i457j0i8i13i30.11014j0j7&sourceid=chrome&ie=UTF-8.

8. Office of Foreign Assets Control – Sanctions Programs and Information, U.S. Department of the Treasury, https://home.treasury.gov/policy-issues/office-of-foreign-assets-control-sanctions-programs-and-information (last visited Nov. 6, 2020).

9. These coverages should be in addition to other common coverages applicable to the insured's risks, such as coverage for PCI fines and penalties; technology errors and omissions; various costs associated with data breaches, including costs for voluntary notification, crisis response, and credit monitoring; and all other reasonable costs incurred.

Walter J. Andrews *is a partner in the firm's insurance coverage group in the firm's Miami office. Walter's practice focuses on complex insurance litigation, counseling and reinsurance arbitrations and expert witness testimony. He can be reached at +1 (305) 810-6407 or wandrews@HuntonAK.com.*

Andrea DeField *is counsel in the firm's insurance coverage group in the firm's Miami office. Andrea has dedicated her career to helping clients manage risk and maximize insurance recovery. She can be reached at +1 (305) 810-2465 or adefield@HuntonAK.com.*

William P. Sowers Jr. *is an associate in the firm's insurance coverage group in the firm's Richmond office. He can be reached at +1 (804) 344-7974 or wsowers@HuntonAK.com.*