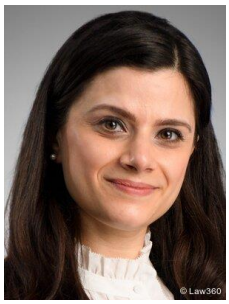
LAW360

Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

How The Rise In Ransomware Is Affecting Business Insurance

By **Marialuisa Gallozzi and Josianne El Antoury** (April 25, 2022, 10:22 AM BST)

Marialuisa Gallozzi



Josianne El Antoury

The U.K. has taken a prominent role in warning individuals and organizations about threats in cyberspace and recommending preventive measures to address such threats.

First, the U.S. Cybersecurity and Infrastructure Security Agency, or CISA, joined with cybersecurity authorities in the U.K., Australia and the U.S. to issue a joint cybersecurity advisory warning about the increasing diversity of tactics used by threat actors and targets of the threats.

Second, the U.K. National Cyber Security Centre, or NCSC, recommended specific steps for organizations to avoid such attacks, including checking the existence and functionality of fundamental cyber controls and including accelerating implementation of cybersecurity improvements.[1]

Insurers in the U.S., U.K. and EU insurance markets are responding to the unprecedented increase in global ransomware attacks by scaling back coverage and increasing premiums.

Insurance broker Marsh reports that as a result of the frequency and severity of ransomware attacks, the cost of cyberinsurance cover rose by 92% in the U.K. and 130% in the U.S. markets in the fourth quarter of 2021 compared with the same period in 2020.[2]

This article describes these market developments and provides guidance to policyholders on managing the ransomware risk.

The Current Cyberinsurance Landscape

Insurers are still willing to write cyber risk insurance, but it has become a lot more expensive and insurers are charging more for less coverage.

At one extreme is AXA SA, a cyberinsurer, which announced that it will no longer cover ransomware payments in new cyber policies issued to French policyholders. France suffered an estimated $5.5 billion in ransomware losses in 2020, surpassed only by ransomware losses in the U.S.

AXA said the decision was in response to concerns raised by French justice and cybersecurity officials during a senate roundtable in Paris in April 2021.

The Dutch government is apparently considering legislation to bar insurers from covering ransomware payments by corporate policyholders, according to Business Insurance.[3]

Hiscox Ltd., a U.K. insurer, has decided not to cover certain kinds of policyholders. It is not renewing its larger premium cyber business and instead is focusing its cyber underwriting on customers with lower revenues in the retail sector.

Insurers have also responded to the dramatic increase in ransomware incidents by reducing the limits and refining the scope of coverage provided by their cyber risk policies.

Chubb Limited, a cyberinsurer, has introduced several restrictive endorsements. Chubb's marketing materials[4] explain that Chubb's Ransomware Encounter endorsement adopts a combination of:

- Sublimits, which cap the insurer's liability below the aggregate policy limit;
- Increased insured retentions; and
- Coinsurance, a percentage of loss payable by the insured even after it has paid the retention.

Chubb's marketing materials also explain that Chubb's new neglected software exploit endorsement adopts a sliding scale of risk-sharing with the insured when the insured fails to update a known software exploit. That is, the longer an insured has "neglected," in the insurer's words, to update the software that was exploited in a cyber incident, the lower the insurer's limit of liability and the higher the insured's share of the loss arising out of the cyber incident.

Lloyd's of London has also introduced Lloyd's Market Association model cyberwar and cyber operation exclusion clauses for cyberinsurance policies.[5]

Insurers across the board are also applying stricter underwriting criteria for cyberinsurance policies. For example, many are requiring policyholders to have multifactor authentication in place.

In assessing risk, insurers are requiring more detailed submissions from prospective insureds, including "vulnerability scans" of all systems connected to the insured's network. This means that the underwriting process takes longer and that insureds should be prepared for more scrutiny of their cybersecurity protections. Although this process sounds burdensome, it is possible that it can help insureds improve their cybersecurity.

The Outlook for Ransomware Insurance Coverage

Ransoms are often demanded by criminal enterprises that may operate in countries subject to sanctions. An insured can mitigate risks by taking sanctions laws into consideration before paying a ransomware demand.

U.S. companies are generally prohibited from engaging in any financial transactions with persons identified on the U.S. Treasury Department's Office of Foreign Assets Control, or OFAC's, Specially Designated Nationals and Blocked Persons — SDN — List, and with those located in certain sanctioned

countries or territories.

As OFAC indicates in its updated advisory on sanctions risks for ransomware payments,[6] it would consider a ransom paid to a sanctioned person or sanctioned country to violate U.S. law, even if the victim of the ransomware attack was unaware that an SDN or sanctioned country or territory was involved. If the victim reports the payment to law enforcement, however, this would be considered a "significant mitigating factor when evaluating a possible enforcement outcome."

A victim should also look beyond the immediate recipient of the payment. Notably, in September 2021 OFAC levied its first sanction on a Russian-operated virtual currency exchange, SUEX OTC, SRO that facilitated ransomware payments. The currency exchange was found to have facilitated financial transactions involving illicit proceeds from at least eight ransomware variants; 40% of its transaction history involved illicit actors. OFAC's actions signal a broader focus on intermediaries that facilitate ransomware attacks.

The U.K and EU also maintain sanctions regimes in relation to certain designated persons and entities, which operate similarly to the U.S. SDN List sanctions noted above.

In contrast to the U.S. sanctions, a ransomware payment should not as a formal matter trigger a breach of U.K. or EU sanctions if the U.K. or EU person involved in making the payment conducted adequate sanctions-related due diligence, but despite that diligence it was subsequently determined that the funds in question ultimately were made available to a sanctioned person or entity.

Nevertheless, as a practical matter similar sanctions-related compliance and due diligence measures would typically be valuable from a U.K. and EU standpoint, as compared to the U.S. sanctions.

The U.K., U.S. and Australia CISA joint report provides technical details regarding the observed behaviors and trends of ransomware actors, mitigation recommendations for network defenders to reduce their risk of compromise by ransomware, and step-by-step advice for responding to ransomware attacks. The cybersecurity authorities in these jurisdictions "strongly discourage paying a ransom to criminal actors," because paying the ransom not only promotes the ransomware business model, but also does not guarantee recovery of the victim's files.[7]

The NCSC has in fact urged U.K. regulators to consider prohibiting insurance coverage for ransomware payments as a means of deterring ransomware attacks. In hearings in March before the U.S. House Judiciary Committee, participants discussed whether making ransom payments illegal would expose the victims of ransomware to a "third extortion" when a cybercriminal could threaten to disclose the ransom payment.

What the Cyberinsurance Trends Mean for Policyholders

As a result of the changing landscape, policyholders should be aware that some insurers may more readily reserve their rights on ransomware claims and force the insured to act as a prudent uninsured until the insurer makes its coverage determination. Where time is of the essence, a policyholder might have to choose:

- To pay the ransom but risk the ransom being uninsured; or

- Not to pay the ransom if the insurer won't cover it and risk significant business interruption and other losses when the threat actor acts on its threats.

In this environment, policyholders can take certain steps to manage the ransomware/double extortion risk:

- Primary risk mitigation is the first step. For example, a firm's chief information security officer or other IT personnel should be routinely engaging in prophylactic IT security measures such as system vulnerability scans or penetration testing — whether or not required by a cyberinsurance renewal application. Indeed, in its recent advisory, OFAC explicitly references the U.S. Cybersecurity and Infrastructure Security Agency's September 2020 Ransomware Guide[8] as containing best practices and recommendations to reduce the risk of extortion by threat actors.

- Fully engaging in the insurance underwriting process might be helpful in improving a firm's cybersecurity. In any event, taking steps to meet the insurer's specific IT security standards may be necessary to secure the broadest possible cyber coverage. The prospective insured must be careful, however, to have appropriate confidentiality protections in place when sharing detailed cybersecurity information with an insurer.

- Policyholders or their coverage counsel should evaluate their current cyber risk coverage now, to understand the amount and scope of coverage currently available and the notification requirements, including any applicable insurer preapproval requirements for vendor selection, in the event of a cyber incident. They should discuss any gray areas with their brokers or counsel, in case clarified wording might be prudent at renewal.

- Policyholders or their coverage counsel should also inventory other current lines of insurance, including property and business Interruption, errors and omissions, directors and officers, crime, and kidnap and ransom policies, to assess potential paths to coverage in the event of a ransomware attack. In the U.K. particularly, property insurers have taken steps to eliminate what they referred to as "silent cyber." Nonetheless, other traditional property/casualty insurance policies, including general liability and property damage/business interruption policies, should still be analyzed for any remaining coverage potential.[9]

- Finally, it will be prudent to start the renewal process earlier than usual to allow sufficient time for any enhanced underwriting requirements and to evaluate any new policy wordings, even if renewal pricing might not be available until closer to the renewal date.

Marialuisa S. Gallozzi is a partner, and Josianne El Antoury is an associate, at Covington & Burling LLP.

[1] NCSC: "Actions to be taken when the cyber threat is heightened." Jan. 17, 2022.

[2] Law360: "CyberInsurance Jumps 92% In U.K. As Ransomware Spikes." Feb. 2, 2022.

[3] Business Insurance - Dutch government mulls insurer ransomware payment ban.

[4] Chubb: Cyber Enterprise Risk Management.

[5] Lloyd's Market Association Bulletin, Nov. 25, 2021.

[6] Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments. See also Covington's Inside Privacy blog for a commentary on the Updated Advisory.

[7] For an in-depth look at the CISA joint report, see the Covington Alert: "CISA Issues Joint Cybersecurity Advisory on 2021 Ransomware Trends and Recommendations."

[8] Ransomware Guide September 2020.

[9] Covington Alert: "The Noise About "Silent Cyber" Insurance Coverage."