# WINTER IS COMING: THE HBO HACK, RANSOMWARE ATTACKS, AND CYBER EXTORTION COVERAGE

Date: 8 January 2018

**U.S. Insurance Coverage Alert**

By: Jeffrey J. Meagher

Cyber extortion and ransomware attacks made headlines across the globe this summer, but the cyber attack at HBO stands out due to the size of the ransom demanded ($6 million). The HBO hack highlights the importance of one of the lesser known areas of cyber insurance: cyber extortion coverage. Here's what you need to know about the HBO hack, ransomware attacks, and cyber extortion coverage, including best practices and potential pitfalls for companies exposed to this growing cyber risk.

## THE HBO HACK

In July, an anonymous hacker who called himself "*Mr. Smith*" and "*Little Finger*" claimed to have stolen 1.5 terabytes of confidential information from HBO, including unreleased *Game of Thrones* episodes, and demanded a multimillion-dollar ransom payment to prevent its release. HBO reportedly responded by offering to pay the hacker a $250,000 "*bug bounty*" for discovering a flaw in its cyber security defenses as a "*show of good faith*" while it assessed the situation. The hacker has since released videos, emails and other sensitive information online.

The HBO hack comes on the heels of the WannaCry virus and other so-called "ransomware" attacks that spread across the globe this summer, but the HBO attack stands out, in part, due to the size of the ransom demanded. The hacker or group of hackers behind the HBO attack demanded "*our 6-month salary in bitcoin*" and claimed to earn $12 million to $15 million dollars a year, which translates into a ransom of at least $6 million. Unfortunately, high-dollar extortion demands may be a new trend. According to a Wall Street Journal article, one group of hackers tracked by cybersecurity investigators began by demanding approximately $50,000 from casinos and energy companies in exchange for not publishing sensitive information, but that same group is now demanding as much as $620,000. [1]

## CYBER EXTORTION COVERAGE

The size of the ransom demanded has significant insurance implications because most cyber policies provide cyber extortion coverage subject to a deductible or self-insured retention (and sometimes sublimits). Although the specific policy wording varies from policy to policy, many cyber policies provide coverage for extortion-related expenses and payments paid by the policyholder as a result of a cyber extortion threat. A sample insuring agreement is shown below:

> The Insurer shall pay Extortion Expenses and Extortion Payments actually paid by the Company as a direct result of a Network and Data Extortion Threat that occurs during the Policy Period, that is reported to the insurer in accordance with [the policy's notice provisions], and to which the Insurer consents in writing prior to the offering of such reward.

"*Extortion Expenses*" are defined to mean *"the reasonable and necessary expenses incurred by the policyholder that are attributable to a Network and Data Extortion Threat*," but certain types of expenses may be excluded from that definition, including "*any costs or expenses to correct any deficiencies, identify or remediate Software errors or vulnerabilities, or costs to update, replace, modify, upgrade, restore, maintain or improve any security system of Computer System of the Company*."

> "Extortion Payments" are defined to mean:
> monies paid to a third party whom the Company reasonably believes to be responsible for a Network and Data Extortion Threat; provided that:
>
> 1. the Insurer's prior written consent is obtained prior to making such Extortion Payments; and
> 2. such extortion Payments are made to terminate the Network and Data Extortion Threat.
>
> "Network and Data Extortion Threat" is defined to mean:
> a credible threat or connected series of credible threats made by a natural person to an Insured where such natural person:
>
> 3. introduces or threatens to introduce Malicious Code into the Computer System of the Company;
> 4. interrupts or threatens to interrupt the Computer System of the Company through a Denial of Service Attack;
> 5. disseminates, divulges or improperly utilizes or threatens to disseminate, divulge or improperly utilize any Non-Public Personal Information or Confidential Corporate Information in any format; or
> 6. engages in Cyberterrorism.
>
> "Confidential Corporate Information" is defined to mean:
> Corporate information, in any format, that has been provided to the Insured by a third party which is not available to the general public and is subject to a mutually executed written confidentiality agreement or which the Insured is legally required to maintain in confidence.

## BEST PRACTICES AND POTENTIAL PITFALLS

Cyber policies typically require a policyholder faced with a cyber extortion threat to notify its insurer and seek its insurers' consent before making any extortion-related payments. Although the policy language quoted above does

not expressly provide that the insurer's consent may not be unreasonably withheld, an insurer generally owes its policyholder a duty of good faith and fair dealing, so a policyholder has a very good argument that an insurer may not unreasonably withhold its consent to a payment that a policyholder believes to be reasonable and in its best interests. That said, a policyholder should try to negotiate policy wording which expressly states that the insurer may not unreasonably withhold its consent. In any event, the larger the ransom payment demanded, the more incentive an insurer has to withhold its consent and contest coverage.

An insurer may also argue that the extortion-related expenses and/or payment fall outside the cyber policy's insuring agreement. An insurer, for example, may argue that a threat to disclose the policyholder's own confidential information (as opposed to third-party information in the policyholder's possession) is not an extortion-related threat within the meaning of the policy. A threat to disclose the policyholder's own confidential information, however, is just as much of a cyber extortion risk as a threat to disclose third-party information in the policyholder's possession. A policyholder such as HBO, for example, would want its cyber insurance to provide coverage for any extortion-related expenses it incurs in connection with a threat to disclose its own creative content. Accordingly, companies purchasing cyber extortion coverage should try to negotiate policy wording that clearly covers this type of threat regardless of whether the information at issue is third-party information.

The requirement that an extortion threat be made by a "*natural person*" may also prove problematic. For example, it may be difficult to prove that a threat was made by a "*natural person*" when the identity of the hacker or group of hackers is unknown, as is often the case. An insurer may also argue that a cyber attack sponsored by a nation-state does not satisfy the "*natural person*" requirement. It should not matter whether the "*person*" making the threat is a nation-state, a hacktivist organization, or a line of computer code, but the "*natural person*" requirement may cause unnecessary problems that can be avoided by removing that language during the policy negotiation process.

It is also important to remember that a cyber extortion attack may trigger other types of coverage, including business interruption coverage. Business interruption coverage can compensate your company for lost revenue or earnings resulting from a cyber attack, including a cyber extortion attack. This can be important coverage if the cyber extortion attack threatens to shut down your company's computer systems or otherwise interferes with normal business operations.

## CONCLUSION

A company that understands the potential pitfalls associated with cyber extortion coverage can put itself in the best possible position to secure coverage in the unfortunate event that it falls victim to cyber extortion. Given the dramatic increase in ransomware attacks and other forms of cyber extortion over the past few years, and recent increases in the amount of money demanded, companies exposed to this risk would be wise to think about their cyber extortion coverage sooner rather than later.

## HOW OUR CYBER INSURANCE PRACTICE CAN HELP

K&L Gates provides cyber insurance legal services to corporate clients around the globe. Our cyber insurance

coverage practice is comprised of professionals with extensive experience in a wide range of cyber insurance matters, including:

- cyber insurance policy reviews and counseling before and after placement
- recommendations on policy enhancements
- "coverage gap" analyses
- pursing insurance coverage in litigation/arbitration
- helping clients mitigate risk and loss through a coordinated approach to cyber insurance and other insurance products

**Portions of this alert were published in Risk Management Magazine.*

---

[1] Robert McMillan, Hackers' Latest Weapon: Cyber Extortion, WALL STREET JOURNAL, Sept. 13, 2017 https://www.wsj.com/articles/hackers-latest-weapon-cyber-extortion-1505295003.

## KEY CONTACTS

**JEFFREY J. MEAGHER**
PARTNER

PITTSBURGH
+1.412.355.8359
JEFFREY.MEAGHER@KLGATES.COM



 