## Insurance Recovery and Counseling

# Cyber and Kidnap/Ransom Insurance Should Respond to Massive Global Ransomware Attacks in More than 100 Countries - But Policyholders Must Consider Complex Issues Surrounding the Reporting and Consequences of These Attacks

By: Matthew L. Jacobs

A highly dangerous type of ransomware, or malware, infected thousands of systems in more than 100 countries on Friday May 12, 2017. The attacks do not seem to be over as of Monday, May 15, as many new attacks – possibly from different forms of ransomware – have been reported in Japan, Taiwan and South Korea. The initial ransomware attack was caused by something known as "WannaCry" or "WanaCyrpt0r 2.0" and is reported to exploit a security flaw in Microsoft software found by the National Security Agency for its surveillance toolkit. Although Microsoft, once warned by the NSA of the flaw, took steps to warn users of the problem last week, many systems remained open to attack, either because system administrators failed to apply the recommended patch or because they used outdated software. *Washington Post*, "Nations Race to Contain Hacks," May 14, 2017, at A1. Ransomware locks down a user's access to computer systems, data and other information, and threatens to continue this lock down, until it is removed or neutralized through the use of a decryption key. The hacker then demands the payment of a ransom, in bitcoin – which is typically untraceable – in exchange for the provision of the decryption key or other means of removing the malware. Here, the initial ransom demanded was only $300 or slightly more. Because these events trigger so many complex insurance coverage considerations, as described herein, a policyholder who has been the victim of a ransomware attack may wish to consider contacting experienced insurance coverage counsel as soon as the attack has been recognized.

Prior to Friday's attack, ransomware had been identified as the number one cybersecurity risk facing computer and data storage systems by numerous international agencies, insurers and law enforcement groups. For example, in October 2016, Beazley, a large cyber insurance underwriter, reported that there had been 1437 data breaches suffered by Beazley policyholders during the first nine months of 2016 whereas there had been only 931 such data breaches for the same time period in 2015. *Beazley Breach Insights,* October 2016. During the first nine months of 2016, a hack or malware accounted for the highest percentage of cyber incidents in the higher education (46%), financial services (39%) and healthcare (19%) industry sectors. *Beazley Breach Insights.* The FBI estimated that ransomware payments in 2016 totaled more than $1 billion (compared with only $24 million in 2015). More than 72% of Australian businesses were hit by ransomware attacks in 2015 (Australian Government 2015 Cyber Security Survey). The threat of ransomware, and how cyber insurance products would respond to ransomware attacks, was the subject of a joint presentation by Jenner & Block and Willis Towers Watson on February 2, 2017 in Willis' London offices. A video of the presentations can be accessed at:

Panel 1: click here to access the presentation

Panel 2: click here to access the presentation

There were several high-profile ransomware incidents in the United States in 2016 affecting educational institutions and hospitals, such as the Los Angeles Valley College District in December 2016 ($28,000 in bitcoin demanded), and the Hollywood Presbyterian Medical Center in February 2016 ($17,000 in

bitcoin demanded). Even the Seehotel Jaegerwirt in Austria saw a ransomware attack pursuant to which hotel guests were remotely locked out of their rooms in January 2017. In each case, the ransom demanded (which has been, on average, less than $1,000) was well below the applicable self-insured retentions (SIR), or deductibles, in the relevant cyber policies.

Most current versions of cyber insurance policies provide some form of “extortion” coverage, which is what a ransomware attack initially generates: an extortionate request for the payment of money. A typical cyber insurance policy might include the following coverage provision and definitions:

First Party Coverages

Cyber-Extortion

> The Insurer will reimburse the Insured Company for cyber-extortion expenses that the Insured Company incurs resulting from a cyber-extortion threat.

Cyber-Extortion Expenses

1. Reasonable and necessary money, property or other consideration surrendered as payment on behalf of the Insured Company to which the Insurer has consented, such consent not to be unreasonably withheld, in order to prevent or limit a cyber-extortion threat; and
2. The reasonable and necessary costs agreed to by the Insured Company and the Insurer to conduct an investigation to determine the cause and scope of a cyber-extortion threat.

Cyber-Extortion Threat

A threat or connected series of threats to commit an intentional attack against a network first made during the policy period to:

1. Disrupt the Insured’s business operations;
2. Alter, damage or destroy data stored on the network;
3. Use the network to generate and transmit malware to third parties;
4. Deface the Insured’s website; or
5. Access, distribute, remove, alter, damage or otherwise misuse personally identifiable information, protected health information or confidential business information stored on the network,

made by a person or group, whether acting alone or in collusion with others, demanding payment or a series of payments in consideration for the elimination, mitigation or removal of the threat.

Cyber Security Breach

> Any unauthorized access to, use or misuse of, modification to the network and/or denial of network esources by attacks perpetuated through malware, viruses, worms and Trojan horses, spyware and adware, zero-day attacks, hacker attacks and denial of service attacks.

Assistance and Cooperation

> The Insured will take all reasonable steps to limit and mitigate any loss arising from any third party wrongful act or first party incident for which coverage may be or is sought under the Policy. To the best of its abilities, the Insured will do nothing that in any way increases the Insurer’s exposure under the Policy or in any way prejudices the Insurer’s potential or actual rights of recovery.

The above-listed provisions, definitions and conditions raise numerous considerations for a policyholder: initially, before a ransom payment can even qualify for coverage under the above definition, the policyholder must inform the insurer of the ransom demand and must obtain the insurer’s consent (which cannot be “unreasonably withheld”) before paying the ransom. What if the insured does not want

to pay the ransom, and is, in fact, being encouraged by local law enforcement authorities not to pay the ransom? If further damage results from not paying the ransom, will a cyber insurer refuse to pay for that damage and business interruption? Do insurers want to encourage policyholders to ignore the direction of law enforcement authorities? What if the insurer, upon investigating the matter, directs the insured to pay the ransom, but the insured refuses for good reason? Is the failure to pay a ransom going to be considered a "failure to mitigate" under the Assistance and Cooperation provision? What happens if, upon informing law enforcement authorities, those authorities seek to investigate the circumstances, seize the victim's computer data and information to conduct forensics analyses and also question the victim's personnel? Will that lead to further business interruption and extra expense, triggering a separate first party coverage provision, and the inability to provide health care services, or to register students for classes? Is that something that the policyholder and insurer should consider and weigh in determining whether or not to pay the ransom? After some initial ransomware attacks, law enforcement authorities recommended against the payment of ransom, as such payments might only encourage more attacks and might not stop the hackers from launching new attacks. More recently, however, some law enforcement agencies have taken a neutral position and have informed victims that they should, or should not, pay the ransom based on their own analysis and how their business operations would be impacted by either scenario.

Finally, when does a "cyber-extortion threat" become a "cyber security breach"? A cyber security breach in most cyber policies triggers both Business Interruption and Extra Expense, and Data Recovery, first party coverage parts. This question raises a separate host of considerations.

Policyholders will carefully want to consider whether or not to report such attacks, even if the ransom paid (or demanded) is far less than the applicable SIR or deductible, as the failure to do so could result in adverse consequences in the future. (Because the SIR or deductible in most kidnap and ransom policies is often much lower than that in a cyber policy, the notice analysis could be far simpler and coverage might be available much sooner).

Also, some ransomware may remain dormant on a user's system even though the initial ransom is paid and the decryption key has been used to unlock the system's data. Moreover, as appears to be the case with the WannaCry attack – or even new attacks based on different forms of ransomware -- it would appear that the global attacks did not start and end on Friday, May 12, but are continuing as of Monday, May 15, when people returned to their offices.

If the initial ransomware attack was not reported to the insurer in a timely fashion, and a second attack takes place six months later and is only then reported to the insurer, the insurer may assert a "late notice" defense to avoid coverage of the damage from the second attack – which could be far worse – if the two attacks were the result of the same form of ransomware or if the two attacks were "related" because the second attack can be traced back to the malware infection that took place at the time of the first attack. Also, if there is a new insurer on the risk at the time of the second attack, and the first attack was not disclosed as part of the application process for the second cyber policy, the insurer might assert that the failure to disclose the first attack represents a material non-disclosure of a potential risk, which, conceivably, might lead the insurer either to seek to rescind the cyber policy or, at the very least, deny coverage for the losses arising from the second cyber attack.

Thus, notice to the current insurer could be critical, and disclosure of a ransomware attack is also an important consideration when applying for a new cyber insurance policy or renewing an existing policy. Policyholders, therefore, need to be vigilant and well-informed when addressing issues of notice of a current attack or disclosure in the context of a cyber insurance (or other) application. Moreover, the legal standards governing the scope of a policyholder's notice and disclosure obligations at the time of a cyber attack or cyber insurance policy application can vary widely depending upon the state's law that would apply at the time a claim is made.

All of these issues demonstrate that a policyholder must carefully consider all the complex issues surrounding post-cyber attack actions and that the guidance of experienced insurance counsel, as well

as insurance brokers, may be necessary to preserve insurance coverage in the face of such events.

## Contact Us

**Matthew L. Jacobs**

mjacobs@jenner.com | Download V-Card

**Visit Jenner.com**