THREE PRACTICAL CONSIDERATIONS WHEN EVALUATING YOUR CYBER EXTORTION COVERAGE

Date: 30 January 2018

U.S. Insurance Coverage Alert

By: John Hardin

Cyber crime has increased significantly over the past several years, with no indications that the annual increases will stop or even slow down. Many analysts predict that global ransomware "damages" will exceed $5 Billion in 2017, a 1500% increase from the $325 Million in damages that ransomware caused in 2015. [1] The increase in cyber crime activity is likely to continue with costs to the global economy reaching $6 Trillion on an annual basis by the year 2021. [2]

Ransomware (also known as cyber extortion) is a significant part of this increased activity. Ransomware is a type of malware that prevents or limits access to a computer system by locking the computer system's screen or the users' files until a ransom is paid. Modern ransomwares (generally referred to as crypto-ransomware) encrypt certain file types and demand a ransom in exchange for the decrypt key. [3] Ransomware is a "preferred" method of cybercriminals and consistently accounts for a large portion of cyber incidents ranging anywhere from one-third to one-half of recent cyber incidents. [4] As the WannaCry and Petya/NotPeyta/Nyeta/Goldeneye attacks and the release of the Vault 7 documents have shown, ransomware attacks are growing and being deployed and coordinated on a global scale, meaning that their sophistication and cost on the global economy continue to increase.

Cyber extortion coverage is a common part of cyber insurance policies, although it may also be found in some crime policies. The cyber extortion coverage within a cyber policy generally provides coverage for "payment" and related expenses. "Payments" are the monies paid to the perpetrator to unlock your system, unencrypt your data or call-off a denial of service attack. The coverage for related expenses provides payment for professional services such as forensic computer scientists to stop the current attack from continuing or to prevent similar attacks in the future, attorneys, and crisis management firms.

With approximately seventy (70) insurance companies drafting their own cyber policies, the variations of policies related to cyber extortion is extensive. Here are three practical considerations that prudent risk managers should evaluate when analyzing if their cyber extortion coverage adequately transfers their company's risk.

First, what actions does the policy require the policyholder take before paying the ransom? Does the policy require notice to the insurance company before the policyholder pays the ransom or does the policy allow the policyholder to pay the ransom and seek reimbursement? If the policy requires notice, does the policy also require that the insurance company consent before the ransom is paid? Planning to comply with notice and consent provisions relating to cyber extortion includes placing directions for such notice in the company's cyber incident response plan and ultimately accomplishing it during a cyber event when communication and time is at a

premium. If the policy requires notice (and/or consent) before the ransom is paid and the policyholder does not comply, carriers will argue that the failure is a material breach and relieves the insurance carrier of any obligations under this portion of the policy.

Moreover, notice and consent provisions can delay the process of resolving a cyber extortion incident, which can be critical for certain industries. Take the healthcare industry—the number one target for ransomware attacks—as an example. At any given moment, a healthcare facility may be performing any number of procedures that are dependent on an active operating system and network and which could be life-threatening if the procedure is immediately and unexpectedly halted by a failure of the computer system as a result of a ransomware attack. Adding in any type of delay during a ransomware attack to inform the insurance company and receive permission to pay the ransom increases the risk that something tragic may happen. Companies in similar situations should negotiate on the front-end for as much control as emergency situations may require, with notice and consent to follow.

Second, does the policy limit coverage to attacks from individuals as opposed to state actors? Some cyber policies require that the cyber extortion be made by a "natural person," meaning that the policy may not cover attacks by nation states. While cybersecurity experts can determine the identity of the perpetrator of some attacks, they will not be able to do so for all attacks. If the insuring agreement contains any limitation on coverage based on who performed the acts, insurance carriers may argue that it is the policyholder's burden to prove that any attack fits into the limited definition before the carrier has to honor its obligations.

Third, does the policy cover payments in all forms of digital currencies? Some policies cover only "monies" paid to stop a ransom attack. Does the definition of "monies" in your policy include a broad definition of digital currencies such that it would cover all digital currencies such as virtual currencies, crypto-currencies, and any other type of emerging digital currency? Bitcoins are the currently preferred method of payment by cybercriminals because they are anonymous. But, bitcoin is not a form of currency backed by any nation state, and it is an unresolved question whether bitcoin or other crypto-currencies are considered "monies". Furthermore, if the cyber extortion coverage broadly defines "monies" to include all digital currencies—including, for example, digital fiat currency—policyholders may find it useful to review how other coverages define "payments" (such as "transfer of funds" under social engineering coverages) to ensure all definitions are equally broad to preclude an argument that some coverages did not include all forms of digital currencies.

Cyber extortion is only one of many types of cyber risk. Because cyber risk will increase over the foreseeable future, prudent policyholders would do well to explore the cyber insurance market and, when possible, to negotiate the broadest coverage available. Most cyber policies are negotiable as to critical coverages, which can lead to effective risk transfer and enhanced cyber risk management.

This article was originally published by Bloomberg BNA on January 26, 2018.

---

[1] https://www.csoonline.com/article/3153707/security/top-5-cybersecurity-facts-figures-and-statistics-for-2017.html.

[2] https://www.advisenltd.com/2016/09/14/report-predicts-costs-up-to-6-trillion-due-to-cybercrime-by-2021/

[3] *See, e.g.,* https://www.trendmicro.com/vinfo/us/security/definition/ransomware

[4] *Compare* http://www.hackmageddon.com/2017/08/24/july-2017-cyber-attacks-statistics/ *with* https://www.ponemon.org/local/upload/file/Ransomware%20Report%20Final%201.pdf

