Client Alert: WannaCry Cyber Attack

You may have been impacted by the worldwide WannaCry ransomware attack and like it or not the attack will continue to propagate in a different and, possibly, more malicious form.

Aon Cyber Solutions is ready to help you respond to the ongoing massive worldwide ransomware attack (and prepare for the next one).

From a risk management standpoint, Aon can assist in prioritizing the financial statement impact of the cost-benefit analysis with respect to the following:

Building an incident response plan in advance of a cyber incident is directly correlated with a lower total cost of risk

- Identification of an internal response team including: industry leading attorneys, forensics, crisis management, law authority, internal and external crisis management/external communications, and insurance professionals.
- This pre-identified and engaged response team allows the team members to benefit from knowing the organization and issues in advance of the incident to facilitate quicker, more accurate, more coordinated and more comprehensive responses.
- Adequate back-up systems allow organizations to continue functioning despite the malware, in this case called "WannaCry," which locks out users and threatens to destroy data unless the victim pays a ransom to decrypt the data.
- In addition to the insurance considerations set forth below, there are a number of critical decision points facing affected organizations, including whether to pay the ransom, how to comprehensively assess and remediate any damage done, other parties to include in this process, and what actions may need to be taken to comply with applicable law. Actions that companies take today may have lasting consequences long into the future.
- European Union General Data Protection Regulation becomes effective May 25, 2018. A cyber readiness assessment now can help prepare the organization on an Enterprise Risk Management level.

We're here to empower results

Kevin Kalinich
Global Practice Leader
312.281.4203
Kevin.Kalinich@aon.com

Christian Hoffman
National Practice Leader
212.441.2263
Christian.Hoffman@aon.com

Stephanie Snyder
National Sales Leader
312.381.5078
Stephanie.Snyder@aon.com

Stephanie Dingman
Senior Vice President and Team Leader
312.381.5146
Stephanie.Dingman@aon.com

Brent Reith
Senior Vice President and Team Leader
415.486.7162
Brent.Reith@aon.com

Eric Seyfried
Senior Vice President and Team Leader
212.441.1406
Eric.Seyfried@aon.com

From an insurance standpoint:

Cyber ransom, in this case to address a ransom demand of $300 (to be paid in Bitcoin) for malware called "WannaCry," can be included in many cyber insurance policies, subject to the following:

- Most policies have a self-insured retention or deductible greater than $300 so the payment would not be covered.
- If the cyber ransom payment is covered by the cyber policy, then the insurer must be notified prior to the cyber ransom payment or the ransom would likely be excluded from coverage.
- If the cyber ransom payment is below the retention, then the insured must still engage the cyber insurer to comply with both the notice and Cooperation Clause.
- The Cooperation Clause requires the insured to engage the insurer in decisions that could impact insurance coverage. Failure to comply could result in a subsequent multi-million dollar business interruption, forensics or liability claim denied because of failure to notice or comply with the cooperation clause for the $300 ransomware payment.
- Aside from ransomware, the larger financial statement issues are business interruption, forensics costs, lost productivity and potential third party liability.
- Coverage for cyber extortion does not mean that there is coverage for business interruption or forensics – they are separate coverages with separate coverage grants.
- Many insurers have "failure to patch" exclusions, which exclude any and all coverage for any and all damages, in the event that the vulnerability had been previously identified and not patched. This particular vulnerability was identified and a Microsoft patch deployed in March 2017.
- Almost all insurers exclude coverage for pirated software implementations. One of the likely reasons for the disproportionate impact on computer systems in Russia, former Russia republics, China, and other Asian countries is the purported high incidence of implementing pirated Microsoft programs and other software, which is not supported by the software vendor. This is another important exclusion.
- Some cyber policies exclude cyber terrorism and cyber war, depending upon the specific policy wording.
- Some cyber policies require the insured to contact law enforcement to obtain approval to pay the cyber ransom.
- There could be potential business interruption and forensics coverage under property policies.
- There could be potential cyber ransom coverage under Kidnap and Ransom policies.
- There could be potential third party liability coverage under professional liability and/or general liability policies.
- Impacted companies should review each of the policies mentioned above, as well as their Director's & Officer's policy. Many cyber policies offer ransom or extortion coverage, which includes the cost of the ransom payment.
- Despite the urge to move swiftly in response to this crisis, we recommend policyholders understand and comply with the cooperation clause and notice provisions of their policies to help preserve their right to insurance coverage.

Despite the urge to move swiftly in response to this crisis, we recommend policyholders understand and comply with the cooperation clause and notice provisions of their policies to insure they preserve their right to insurance coverage.