Client Alert: WannaCry Cyber Attack

The ongoing worldwide WannaCry ransomware attack has demonstrated cyber risk represents a material threat to business continuity and corporate reputation. As the attack continues to evolve, Aon’s Cyber Solutions Network considers key learnings to respond to WannaCry and prepare for the next attack.

From a risk management standpoint, Aon recommend the following actions to improve cyber preparedness

The WannaCry ransomware attack shows that the following activities can be critical to lowering the total cost of risk:

• **Patch Management:** Review the patch management programme, including use of automated patch management tools.

• **Back-ups:** Deploy back-up systems that will allow continued data availability despite the activation of malware (which can attempt to lock out users from data and threatens to destroy data unless the victim pays a ransom).

• **Business Continuity and IT Disaster Recovery:** Review and test current Business Continuity Management and IT Disaster Recovery plans against cyber events (such as ransomware attack) to determine suitability to support operational continuity.

• **Incident Response Planning:** Formation and preparation of an incident response team in advance of an incident to facilitate quicker, more accurate, more coordinated and more comprehensive responses. Critical external team members should include:
  - Legal experts to provide legal and regulatory guidance
  - Digital Forensics vendors to determine the source of infection and causality, affected data, and expedite system remediation
  - Claims preparation experts who are familiar with the rapidly evolving insurance policies and business interruption coverages, to support claims preparation and advocacy

• **Tabletop Simulations / Incident Response Rehearsals:** In addition to the insurance considerations set forth below, companies should conduct tabletop simulations or rehearsals of the Incident Response plans with key decision makers to ensure the plans are appropriate and responsive. Key decisions in this exercise would include whether to pay the ransom, how to comprehensively assess and remediate any damage done, which (if any) other parties to include in this process, and what actions may need to be taken to comply with applicable law.
From an insurance standpoint:

Cyber ransom can be included in cyber insurance policies, subject to the following:

- In the case of “WannaCry”, the ransom demand was for US$300 per machine so only companies with a significant number of machines would incur a ransom loss excess of their policy’s deductible.

- Under most policies, the insurer must be notified prior to the extortion payment being made.

- If the extortion payment is within the deductible, the insured must usually still notify the insurer to comply with both the notice and cooperation clause of the policy.

- Although there is obviously a desire to react swiftly to this type of event, a policy’s notice and cooperation clause normally requires the insured to engage the insurer in decisions that could impact insurance coverage. Failure to comply with the provisions of the clause could result in the insurer denying subsequent forensics costs, liability payments, or business interruption loss that result from the same originating cause or source.

- Aside from the amount of any extortion payment, there is potential for financial impact through business interruption, forensics costs, lost productivity and potential third party liability.

- Coverage for cyber extortion is limited to indemnity for the amount paid to the extortionists. Separate coverage is available for business interruption, forensics costs, lost productivity and third party liabilities.

- Many insurers have “failure to patch” exclusions in their policies, which exclude coverage in the event that the vulnerability had been previously identified and not patched. This particular vulnerability (“WannaCry”) was identified and a Microsoft patch deployed in March 2017.

- Almost all policies exclude coverage for pirated software implementations. One of the possible reasons for the disproportionate impact on computer systems in some countries is the purported high incidence of implementing pirated Microsoft programmes and other software in these territories.

- Some cyber policies exclude cyber terrorism and cyber war.

- Some cyber policies require the insured to contact law enforcement to obtain approval to pay the cyber ransom. In some territories, payment of extortion demands is prohibited by law.

In addition to their Cyber policy, impacted companies should also review other insurance policies such as their Property policy; Kidnap & Ransom and/or Crime policy; Professional Liability and/or General Liability policy; Director’s & Officer’s Liability policy.

- Property policy: there could potentially be business interruption and forensics coverage under Property policies.

- Kidnap & Ransom and/or Crime policy: there could potentially be cyber ransom coverage under Kidnap & Ransom and/or Crime policies.

- Professional Liability and/or General Liability policy: there could potentially be third party liability coverage under professional liability and/or general liability policies.

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