

Managing cyber risks Part 2: cyber liability insurance policies

In part one this trilogy, Browne Baker, a fictitious law firm, aided in highlighting some of the typical deficiencies with IT contracts and the potential dramatic impact on businesses if these deficiencies occur during a cyber incident. Following here, in part two, learn more about the importance of cyber liability insurance policies. And then continue to read part three “business interruption losses”, to learn more.

While writing this article, we got news that a company we know well had fallen victim to a cyber ransom attack. In a state of some panic, the company's directors turned to their cyber liability insurance policy and were disappointed (to say the least) that it did not appear to provide the cover they expected. Not a great place to be.


This is not what cyber liability insurance underwriters want for their policyholders. In many cases, it is not the fault of the insurer but rather the fault of the insured. Many insureds we speak to admit to buying cyber liability insurance without properly reading and understanding the terms of the policy - to satisfy themselves that the policy will respond if their system goes down and they are prevented from functioning properly for a period.

Few buyers of cyber liability insurance policies, particularly small- and medium-sized businesses, carry out scenario planning, a process designed to ensure policy wording reflects the insured's specific exposures and contractual arrangements in the event of a cyberattack. As will be seen later in this article, insurance brokers can and should play a key role in scenario planning as part of an insured's presentation of its risk and the related disclosure process.

There remains an unfortunate reliance by many policyholders on so-called “silent cyber” cover. This can arise where a traditional property or casualty insurance policy appears to provide some cover for cyber-related exposures simply by not expressly excluding it. The Prudential Regulation Authority (PRA) highlighted this issue for insurers in its clampdown on unintended exposures in 2017, following which all Solvency II firms were required to robustly assess their insurance products, particularly in relation to non-affirmative cyber exposures.

There is a wider corporate governance issue here too. The failure of an organisation (in particular, a quoted company) to secure effective cyber liability insurance, could result in stakeholder action against the organisation and potentially a claim on the organisation's Directors & Officers (D&O) policy, with its associated reputational fallout.

The common criticism levelled at cyber liability insurance is the inconsistency of policy wordings. This is likely to be because the main trigger event for a stand-alone cyber liability insurance policy - a “network security failure” or a “data breach” - is often difficult to define, and consequential losses vary dramatically depending on the type of industry impacted. For example, the loss of a pharmaceutical company's intellectual property as a result of a cyberattack may lead to very different consequential losses compared to a retail organisation losing customers' financial data.



Cyber liability insurance is still very much in its infancy as a product type. Other insurance markets, such as space or marine, have had many decades or even centuries to evolve in response to case law on policy wordings. Competition should eventually lead to a convergence in cyber liability insurance policy wordings among insurers, but this could take many years. In the meantime, insureds should look to experienced broking and legal advisers to assist them in reviewing and negotiating policy wordings so that they make the right choice of cover for their businesses.

In the case of our fictitious law firm, Browne Baker (in the scenario outlined in Part 1 of this article), it turns out that there is a disconnect between the cyber liability insurance policy wording and the terms of their IT cloud services contract with Blue Sky. As the cyber incident was caused by the failures of Blue Sky, Browne Baker wanted recompense from them. Unfortunately for Browne Baker, the terms of Browne Baker's contract with Blue Sky were not reflected in Browne Baker's cyber liability insurance policy.

At the time of the insurance placement, Browne Baker was obliged by law to provide a fair presentation of its risk to its insurer, so that the insurer was aware of the precise parameters of the potential risk event. A key component of Browne Baker's presentation of its risk should have been disclosure of the terms of its contract with Blue Sky. Browne Baker's insurer should have been made aware of the limitation of Blue Sky's liability to Browne Baker under its contract, in particular the fact that Blue Sky excluded liability for consequential losses and limited its total liability to the giving of service credits. This unintentional waiver (or reduction) of Browne Baker's insurer's rights of subrogation is an all-too-common mistake that can leave policyholders without cover.

The Insurance Act 2015, however, obliges insurers to work actively with insureds at the placement stage to identify potential circumstances or matters which could result in a claim. Therefore, arguably, the underwriter discussing the risk profile with Browne Baker should have been aware of the law firm's lack of specialist IT knowledge and made allowances in relation to the level of detail that the law firm could provide around how the terms of the Blue Sky contract would impact its insurance cover.

Another potential stumbling block is the claims notification process. Strict adherence to this is usually a condition precedent to the insurer's liability. If a policyholder fails to follow the process correctly and inform the insurer within the appropriate timeframe of any circumstances or event (such as a malware attack) which might give rise to a claim on the policy, the policy may not respond.

There is much debate around the feasibility of a policyholder constantly monitoring for potential cyber events. There is also much debate around the reasonableness of some insurers' terms regarding mitigation of an event or circumstance. These issues could be covered by better placement processes and more accurate policy wording.

So, how are insurers adapting to the changing behaviours of cyber criminals, and particularly ransom demands?

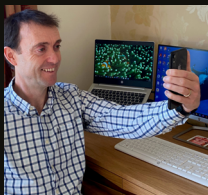
The payment of ransom demands is not, generally, an illegal act. Most cyber insurance policies include cover for extortion payments, but only if the relevant authorities are informed and the insurer's prior written consent is obtained. The situation is very different, however, if there is any suspicion that the money required by the criminals might be linked in some way to terrorism. Under section 17A of the Terrorism Act 2000, any such payments made will be deemed illegal and amount to a criminal act on the part of the insured - and potentially on the part of the insurer, if the insurer is aware of what has happened and fails to inform the authorities.

If a cybercriminal makes a ransom demand, insureds are faced with an invidious choice - pay the ransom demand in return for the release of their data or refuse to pay and see losses and disruption increase. If a ransom payment is made, the insured or its insurer may have the potential to recover the outlay under the Proceeds of Crime Act 2002, but only if the criminals can be identified and caught. It is no surprise that criminals are becoming more and more astute and issuing second ransom demands in return for not releasing stolen data into the public domain.

Understandably, an ethical choice often trumps everything else.

Continue reading our managing cyber risk series in the next article “business interruption losses”.

For more information on the topic, contact our authors:



Michael Ainsworth
Director
London, United Kingdom
michaelainsworth@oconnors.law



Bernard Regan, MSc, MBCS
Partner, Global Forensic & Litigation Services
London, United Kingdom
T: +44 (0)20 7065 7937
bernard.regan@bakertilly.com



Joshua Bates
Solicitor
Liverpool, United Kingdom
joshuabates@oconnors.law



Ben Hobby, FCA, Dip II
Partner, Global Forensic & Litigation Services
London, United Kingdom
T: +44 (0)20 7065 7925
ben.hobby@bakertilly.com



Kathryn Howard
Solicitor
London, United Kingdom
kathynhoward@oconnors.law

Connect with us: bakertilly.com/globalforensics
Connect with us: oconnors.law



The information provided here is of a general nature and is not intended to address the specific circumstances of any individual or entity. In specific circumstances, the services of a professional should be sought.

Baker Tilly US is an independent member of Baker Tilly International, a worldwide network of independent accounting and business advisory firms. Baker Tilly is the trading name of BTVK Advisory LLP, a Limited Liability Partnership registered in England & Wales (registered number OC304572), which is a Baker Tilly US company. The registered office is 5th Floor, 2 London Wall Place, London, EC2Y 5AU, where a list of members' names is available for inspection.
©2020 BTVK Advisory LLP

O'Connors is a trading name of O'Connors Legal Services Limited Company No. 11158860 SRA ID 647864 VAT 292977933