Stepping into the breach
Managing cyber risks with insurance

July 2019
The market for cyber insurance continues to grow\(^1\), as demand increases in the face of the increased frequency of cyber attacks (and the impact of those attacks). Yet there is a recognition amongst regulators, that as the market is still nascent and maturing, underwriting methods require further refinement and policyholders remain unsure as to how to articulate their insurance requirements\(^2\). In addition, recent, high profile disputes between insurer and insured have underlined the importance of understanding the scope of coverage and addressing any critical gaps.

Insureds are beginning to understand the danger of relying on non-cyber insurance policies to cover specific cyber risks:

- will their traditional insurance policies insure business interruption and loss of data caused by a cyber attack?
- do they cover ransom and extortion demands?
- what if the breach came about through unpatched systems or social engineering?
- will they cover the down-stream effects of attacks on operational technology (such as ICS and SCADA systems)?
- what of the costs of restoring systems, forensic investigations, legal fees, customer compensation, damage to reputation and regulatory fines?

Increasingly, companies are becoming concerned whether they are adequately insured for cyber attacks perpetrated by state-sponsored groups.

In this briefing, we build upon our article “Your Questions on Cyber Insurance Answered” (first published in 2016)\(^3\) to explore some of these issues and to address some of the questions insureds should be working through with their brokers and underwriters.

---

Stepping into the breach
Managing cyber risks with insurance

First of all, cyber insurance is in a category of its own. Yes, it is possible that some coverage for cyber losses may be available under existing non-cyber insurance policies. For example, some liability policies may cover claims arising from infringement of intellectual property rights or damage to tangible assets (such as servers, PCs and storage devices).

However, non-cyber policies are becoming increasingly inapplicable to cyber events and may not provide comprehensive cover for key categories of losses, (or even expressly exclude them from coverage). Further, cyber claims on non-cyber policies will be harder to bring as insurers become less inclined to agree to expansive readings of existing policies where cyber is not specified.

Standalone or bolt-on?

Cyber insurance is still largely bespoke, and the type of threats are changing so rapidly, that it is important to read the policy not only in light of current threats, but also in terms of reasonably anticipated future threats. For example, if your policy defines cyber attack as being caused by “a person,” will it cover attacks by bots, or by artificial intelligence (AI)? What about by nation states?

In fact, nation states are increasingly behind cyber attacks, especially against larger, more sophisticated companies and those companies which are part of a country’s critical infrastructure. In addition to potentially not being considered a “person,” nation state cyber attacks may also trigger a clause in their commercial contracts that most people never read: the force majeure exclusion clause (see our force majeure exclusion clause article for more information). These clauses are often mirrored by similarly-worded exclusions in insurance policies that vitiate the cover for losses caused by acts of war, warlike activities and acts of terrorism. Whilst it is true enough that the identity and/or motives of hackers are often difficult to establish with sufficient certainty to engage such exclusions, policyholders can reduce their risk by negotiating express carve-outs to them for losses arising from nation state or terrorist-sponsored cyber attacks (if not possible to negotiate the removal of the exclusion(s) altogether).

If you do not have a cyber-specific policy, it is even more important to make sure that this carve-out exists. There is English Supreme Court authority, for example, confirming that insurance exclusions are to be interpreted in light of the context of the policy as a whole4. This could mean that a war risks exclusion in a cyber policy is less likely to apply to a ransomware attack than the same-worded exclusion in a non-cyber policy, because the essential purpose of a cyber policy is to cover a risk of that nature, whereas the same cannot be said for a property insurance policy. That being said, there is as yet little case law in which cyber policies have been interpreted by the courts, which only emphasises the need to proceed with caution when negotiating the wording of these contracts.

Furthermore, if it is good military strategy not to fight the last war, then it is also good corporate strategy not to insure solely against last year’s threats. For example, a few years ago, not many companies had coverage for ransomware attacks. Now, it is essential. The next generation of cyber attack that may not be sufficiently covered are information warfare attacks. These attacks, for example, release - or purport to release - internal corporate emails showing evidence of crimes or embarrassing activity among senior executives. Some of these attacks may not even involve a hack, so are unlikely to be covered by “traditional” cyber policies.

---

4 Impact Funding v AIG Europe [2016] UKSC 57
At a minimum, what should cyber insurance cover?

There is a lot more to a cyber attack than the malware and the worst case scenario is not the breach, as bad as that can be, but the litigation, regulatory enforcement action, business interruption and reputational damage which ensues. To provide greater certainty and predictability, cyber insurance should cover all these potential losses. More specifically, you should expect dedicated cyber insurance policies to provide an indemnity for:

- breach response costs, which are typically the costs of obtaining expert advice in the immediate aftermath of a breach, in areas such as IT forensics, legal and Public Relations
- regulatory costs e.g. customer notification requirements and obligations to provide credit monitoring services to affected individuals
- liability i.e. your liability to third parties in respect of a data breach for which you are legally responsible
- business interruption e.g. loss of revenue or profit suffered as a result of a data breach
- theft of your money
- ransomware demands
- system restoration following a data breach

In addition, as discussed above, you may want to peer around the corner to make sure the next generation of cyber threats are also sufficiently covered.

What should you be wary of?

As we have already indicated, a cyber policy is not an all-singing, all-dancing risk management solution. Nor are all policies created equal. Watch out for the following in particular:

**Cover for fines and penalties** – most cyber policies purport to provide cover for fines and penalties. Some do so without reservation, whereas others do so to the extent such losses are legally insurable. Regardless of the words used or not used, the enforceability of this cover remains very much open to question, since many jurisdictions will not permit a “wrongdoer” to be indemnified for the consequences of their wrongful acts. Fines and penalties are usually levied based on acts or omissions falling into this category. Some policies go even further by seeking to specify that legal insurability shall be determined by reference to the jurisdiction that is most favourable to the insured – there may be real doubt over whether a court in one jurisdiction will be willing to apply the laws of another in circumstances where public policy issues are concerned.

**Breach response panels** – almost every cyber policy will provide access to a panel of experts in the event of a data breach. Sometimes these experts are “written in” with the expectation or indeed agreement that their services will be used. The question for you is, are you willing to place your trust in those experts in a “bet-the-company” event? If not, you may wish to negotiate the inclusion of your own panel of preferred providers, or seek to ensure that the policy provides you with more freedom of choice as and when an incident arises.
Practical tips

- whilst it is possible to purchase basic cover directly from insurers, you are usually better off using the services of a regulated insurance broker who should recommend suitable cover to you based on a proper risk assessment.
- some providers will offer reduced premiums if you are able to obtain certification demonstrating that your cyber security and business continuity practices are robust e.g. Cyber Essentials, ISO 27001 and 22301.
- ask whether your insurance provider will offer add-on services such as training your staff in cyber security best practice.

Please contact the authors if you would like to discuss any of the issues raised in this document or if you would like to take part in one of our cyber-readiness workshops, wargames or tabletop exercises.

Authors

Michael Bahar  
Co-Head of Global Cybersecurity and Privacy  
T: +1 202 383 0882  
michaelbahar@eversheds-sutherland.com

Craig Rogers  
Partner, IT & Cyber  
T: +44 20 7919 0707  
craigrogers@eversheds-sutherland.com

Naz Gauri  
Principal Associate, Insurance  
T: +44 20 7919 0881  
nazgauri@eversheds-sutherland.com