Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

5 Cyber Insurance Pitfalls To Avoid In The UK

By **Richard Mattick** (October 17, 2018, 4:15 PM EDT)


Richard Mattick

As regular press reports of cyberincidents show, cybercrime and other harmful cyber events are becoming ever more prevalent with the growth of the digital economy. It is unsurprising that cyber risks have been at, or near, the top of the list of worries for corporate boards for some time. Cybercriminals in particular have become more sophisticated, resulting in cybercrime costing the U.K. economy 10s of billions of pounds a year. The recent entry into force of the EU General Data Protection Regulation has created additional potential liabilities arising out of cyberincidents.

Faced with the opportunity to purchase cyber risk insurance to mitigate the damage caused by cyber events, prospective policyholder companies need all the help they can get in order to navigate this increasingly complex part of the U.K. insurance market. We have identified five pitfalls that a company intending to purchase cyber risk insurance will want to avoid.

Is the cyber insurance cover fit for its purpose?

As a threshold issue, a policyholder needs to determine whether the purpose of the insurance will be to smooth out every bump in the cyber risk road or to cushion the impact of "catastrophic" incidents only. This decision will affect issues such as limits and deductibles, the scope of insured risks, and possibly also the lines of coverage purchased. The tack taken will likely depend on the policyholder's confidence in its own systems and its ability to react to any incident, including the in-house resources already available to it.

Next, the policyholder should ideally identify the highest priority cyber risks to be covered, consistent with the purpose already identified, based on the likely severity and frequency of the risks. The first-party and third-party risks covered vary from policy to policy. These losses can result not only from actions by outsiders, but also from deliberate or accidental actions by insiders. They can include:

- Costs of responding to the incident, including costs of crisis management, investigation and notification to those affected by the breach;

- Remediation cost to the policyholder, including blocking off leaks and data restoration;

- Reputational risk (such as public relations costs incurred during the crisis management period);

- Recovery of "time element" losses (extra expense and business interruption) (which could be potentially the most significant item for some businesses, and which can be calculated in different ways);

- Bodily injury/physical damage caused by a hack (which may be excluded in some basic cyber policies, but may be offered in newer specialty policies or endorsements for this "cyber-physical" risk);

- Cyber extortion cover;

- Liability to third parties resulting from the leakage of personal data;

- Liability to third parties for the loss of their confidential information;

- The consequences of regulatory liability for breach, which will include defense costs and payment of fines or penalties where local laws permit.

Are the highest priority risks already covered?

The policyholder should check whether any of the risks and consequent losses that it has identified are already covered by its existing policies. For example, dishonest actions by employees may be covered by a fidelity policy. Similarly, general/public liability policies may also provide coverage, although, increasingly, cyber risks are specifically excluded by such policies. Other potentially applicable policies are errors and omissions, media, directors and officers liability and first-party property. A company should consider if all its lines of coverage align properly, and that poorly coordinated "dovetailing" exclusions do not create coverage gaps for major risks.

Are the available limits sufficient?

The policyholder should consider whether its limits for cyberclaims are adequate, taking into account the likely cost of a potential incident, each type of loss and what level of deductible it can absorb.

The policyholder should also pay careful attention to sublimits, which may reduce coverage for the policyholder's main cyberexposures, in addition to making the administration and presentation of claims more difficult.

Do limitations on scope negate the value of the cover?

Insurance may be subject to some intrinsic limitations: for example, in some jurisdictions, criminal fines and penalties may not be recoverable under an insurance policy as a matter of public policy. In some countries, ransom payments may be unrecoverable from insurers. These and other noninsurable risks may have to be dealt with by means of contractual liability restrictions or vendor indemnifications where possible, or through greater investment in IT security.

The policyholder should review the the exclusions in its cyber insurance contracts to determine what is carved out and whether if would be prudent to explore the availability and cost-effectiveness of separate insurance to cover these risks. For example, the insured's liability for infringement of a third

party's intellectual property (including trademarks, copyrights and patents) may be excluded by cyber insurance policies. Therefore, businesses should explore the availability and cost-effectiveness of separate insurance to cover those risks.

Do the dates fit?

Most cyber risk policies are "claims made" policies (covering claims made or cyber events discovered within the policy period) or "claims made and reported" policies (covering claims made and reported during the policy period). They also typically contain "'retroactive date" wording which may limit coverage to losses arising from an act or omission after a particular date (for instance, the first day of cyber coverage with the insurer). Because cyberbreaches can remain undetected for an extended period of time, policyholders need to negotiate as early a retroactive date as possible.

The end date of the coverage can also vary depending on the wording of the policy. Some policies cover only claims must be made during the term of the policy or a specified extended reporting period after the policy expires. Given that it can take months or even years before a cyberbreach is detected, policyholders with expiring policies could be exposed to losses from cybercrimes if claims do not arise within the specified reporting period and there is no subsequent year's coverage, or if the scope of that coverage has changed. Prospective policyholders should ensure that their policies have an automatic extended reporting period, giving the policyholder more time for a claim to be made, as well as a further, optional, extended reporting period. If these periods are of inadequate duration, policyholders should consider negotiating appropriate extensions.

Richard Mattick is of counsel at Covington & Burling LLP.