LOCKTON

UNCOMMONLY INDEPENDENT

The Sound of Silence

Silent Cyber and what it means for you

Background

Cyber risk is everywhere and as such threatens many lines of insurance. Elements of cyber cover have traditionally been found under policies other than cyber, such as property, kidnap and ransom, or professional indemnity. However, this threat is not always affirmatively addressed within these policies. Insurers in non-cyber markets have not always fully considered the implications of cyber exposures, nor have they tackled the potential aggregation over their various types of policies.

This 'silence' in non-cyber policies does not necessarily mean cover is not there – just that it is not affirmative and coverage cannot be guaranteed, potentially leading to both coverage and claim reporting issues.

The growing size and sophistication of the standalone cyber market and the increased cyber risk, have been additional factors prompting a re-evaluation of cyber-specific risks over various lines of insurance.

Regulatory scrutiny by the Prudential Regulation Authority (PRA) into these risk, and the PRA's requirement that insurers suitably identify, assess and manage their cyber liabilities, were factors in Lloyd's issuing a mandate in July 2019. The mandate required Lloyd's underwriters either to affirm or exclude cyber cover in various lines of insurance. Cyber should no longer remain 'silent'.

Lloyd's published a phased roll-out of the dates by which certain lines must comply. The rolling programmes began with first-party property damage on 1 January 2020 and it continues. There is much talk in the market place currently, as the roll-out applied to professional indemnity policies as from 1 January this year, causing a flurry of activity.

The insurance markets are responding to the Lloyd's mandate in a variety of ways. There are some 'standard' clauses in circulation, but we are finding that insurers are interpreting the clauses in different ways and seeking various wording amendments. There are countless versions of cyber endorsements currently in play, reflecting these differing interpretations, as well as market appetite. The preparedness to affirm or exclude cover is by no means consistent across insurers.

Whilst there is no consistent response at this stage, one thing is clear: it is likely that a policy will not renew as expiring.

Consider the Effect

When faced with a new cyber endorsement, a close analysis of its implication will be critical.

Consider the following:

1. Is the endorsement too broad in what it seeks to exclude?
2. If the endorsement is affirmative in nature, is it affirming all cover or does it remain silent on some?
3. Does the Lloyd's mandate (to affirm or exclude cover) even apply to the particular policy in the first place?
4. Are there new gaps in cover?
5. Does any gap in cover necessitate the purchase of a standalone cyber policy?

There are subtleties associated with many of the cyber endorsements which must be understood in order to make fully informed decisions on cyber risk. It is possible that certain coverages currently available will no longer be available.

As indicated above, the purchase of cyber insurance may be a consideration, as may be a reassessment of limits for any existing cyber cover. Every scenario is different and each situation should be assessed on its facts. (There are, for example, particular risks for technology companies that may be affected by the inclusion of certain endorsements currently in circulation. Further, a consideration of the possible fallout from a ransomware attack on a professional services organisation, will be crucial in understanding the full implication of a proposed cyber endorsement).

The renewal process will take some time and early engagement with your broker is recommended.

Vanessa Cathie
Vice President, Global Professional & Financial Risks
T: +44 020 7933 2478
E: vanessa.cathie@uk.lockton.com

The Lockton Global, Cyber and Technology team works with clients to help protect their business from cyber risks, from ransomware *to phishing, targeted hacks, malware, IP theft and various cyber complexities. Due to the sensitive and confidential nature of such risks, we may have created fictional case studies to demonstrate examples of cyber complexities a client might experience. The case studies are inspired by real matters, however, some facts may have been amended to protect client confidentiality. These case studies do not constitute advice. Please seek appropriate advice before taking any action.*