BEALE&CO

Silent Cyber in Professional Indemnity Insurance

Authors:
Andrew Jones
Ahmed Mian

Date:
December 2020

Silent (or non-affirmative) cyber coverage and the systemic risk it poses is a serious concern for the insurance industry, leading to scrutiny from the Prudential Regulation Authority and prescriptive intervention by Lloyd's. Andrew Jones and Ahmed Mian consider the regulators' concerns, what the industry is doing about it and what the future holds, in particular for Professional Indemnity insurers and policyholders.

Cyber risks encapsulate any risk associated with financial loss, disruption or damage to the reputation of an organisation arising from the failure, unauthorised or erroneous use of its IT systems. These risks can arise from both malicious acts (e.g. cyber-attacks) and non-malicious acts (e.g. infrastructure downtime and accidental loss of data).

Cyber risks are growing in number and public awareness of them is increasing. This comes from the ever-increasing reliance on IT systems by organisations of all types (businesses, defence, education, healthcare, charity etc) and the increased frequency of cyber-attacks on these organisations, against the backdrop of increased regulation. The 2018 introduction of the GDPR, in particular, has widened obligations and potential sanctions on organisations for many types of personal data misuse.

The financial losses that can result are very significant, both first-party and third-party: the costs of specialist IT assistance, third party claims for compensation, business interruption losses, regulatory investigations and penalties, ransomware payments and legal costs, to name but a few. The reputational losses can be even more significant.

The insurance industry has responded with a wide variety of specialist cyber insurance products to provide cover for these exposures (even penalties and fines where legally insurable in the relevant jurisdiction) – and at what are likely to be viewed (in years to come) at very reasonable premium rates. However, while the market penetration for bespoke cyber insurance is increasing, not all businesses yet take it out. When a cyber event occurs, therefore, these insureds cast the net wide to test whether any of their traditional insurance policies might provide cover.

What is *"Silent Cyber"*?

"Silent" or "non-affirmative" cyber cover is the provision, perhaps inadvertently, of cover for cyber risks in insurance policies – typically traditional property and liability policies – through not expressly including or excluding cover for such cyber risks.

This contrasts with "affirmative" cyber cover where such coverage is expressly provided, whether in bespoke cyber risks policies or express coverage and extensions in non-cyber policies.

Why is Silent Cyber a problem?

Silent cyber is problematic for both policyholders and insurers. For policyholders, it can result in uncertainty as to the existence of and extent of their cyber coverage, increasing the risk of disputes with their insurers. Lack of coverage in the event of a cyber event could be an existential threat.

For Insurers, they may have inadvertently given cyber cover without having fully assessed or priced the risk for what can be large claims. Large scale cyber events can also impact organisations worldwide and across multiple lines of business, and give rise to previously unrecognised systemic risk. The potential increase of cyber event-driven

class actions in the UK, which could lead to massive losses, is also a growing (and arguably unpriced for) risk (see our article on the rise of UK cyber class actions here).

What is the insurance industry doing?

The UK market for cyber insurance is relatively young compared to the US market. The PRA, (the UK insurance regulator from a prudential perspective) has warned that if the coverage for cyber risks is not managed well, it could pose a significant risk to the viability of insurance companies and the reputation of the UK insurance industry as a centre for excellence and innovation. These concerns have led to a chain of regulatory and market developments:

November 2016: In light of their concerns, the PRA conducted a cross-industry review, resulting in its "*Dear CEO*" letter to insurers in November 2016. The PRA reported that various areas of improvement were needed, for both affirmative and silent cyber cover. In relation to silent cyber, the PRA found:

- Silent cyber was a clear material risk, yet many insurers were unable to demonstrate robust methods for quantifying and managing this risk.
- The potential for significant cyber insurance losses was increasing with time, from both the awareness of silent cyber cover and the frequency of cyber-attacks.
- There was recognition that insurers would find it increasingly challenging to argue that non-affirmative liability policies did not intend to cover cyber risk given the publicity and awareness of the issue.

***July 2017*:** As a result of its findings and follow-up consultation, the PRA issued a Supervisory Statement in July 2017 setting outs its expectations for underwriting cyber risks. In respect of silent cyber, this required insurers to "*robustly assess and actively manage*" their silent cyber exposure. Insurers were expected to introduce measures that reduced their unintended exposure to cyber risks, such as offering explicit cover and adjusting premiums to reflect the additional risk, introducing robust exclusions and/or attaching specific limits of cover.

***January 2019*:** After a follow-up survey, the PRA issued a further *"Dear CEO"* letter to insurers on 30 January 2019 saying that, whilst some work had been done, more was needed, including in insurers' assessment of their silent cyber exposure. As a result of the continued concerns, the PRA required insurers to develop action plans by the first half of 2019 to reduce their unintended exposure to silent cyber.

***July 2019*:** In its Market Bulletin Y5258, Lloyd's set out its response, mandating that all policies of its members provide clarity regarding cyber coverage by either expressly excluding or expressly providing affirmative cyber cover. In this and in its subsequent Bulletin Y5277, Lloyd's set out a phased action plan by lines of insurance to require these necessary changes by:

- ***January 2020*:** First party property policies.
- ***July 2020*:** Political risks and crime policies.
- ***January 2021*:** PI, D&O, EL/PL and aviation policies.
- ***July 2021*:** Medical malpractice and treaty policies.

In order to comply with the PRA and Lloyd's requirements, insurers have developed revised policy wordings, endorsements and exclusion clauses.

The general observation (and complaint from some brokers) has been that many insurers have elected simply to add blanket cyber exclusions, as opposed to providing affirmative cover and (in doing so) have effectively excluded cover for previously covered perils simply because IT systems are involved at some point in the chain of events – even if not the proximate cause of loss. In defence, one can understand an insurer's desire to push cyber-related risks to the specialist cyber policy market where they can be better identified and priced. The difficulty is in identifying a suitable policy wording which fairly delineates between risks that should really be covered and priced in the specialist cyber market while retaining the cover expected in traditional business lines.

BEALE&CO

INSURANCE

Silent Cyber in Professional Indemnity Insurance

The LMA (the Lloyd's Market Association) and the IUA (the International Underwriting Association of London) have developed a number of cyber-related endorsements for use by their members seeking to delineate this issue across multiple lines of business.

How can silent cyber impact Professional Indemnity Insurance?

Professionals are exposed to cyber risks not least because they often hold and transfer large sums of money and sensitive corporate and personal data. The PRA's review specifically identified that PI insurance policies were particularly likely to be exposed to various degrees of silent cyber risk.

PI policies (not least where required by the relevant professional regulator e.g. the SRA, ICAEW etc) are often written on a broad *"civil liability"* basis for claims arising out of the professional's activities. This wide *"civil liability"* cover is then traditionally limited at some level via express exclusions, such as excluding liabilities associated with EL/PL and D&O risks which are intended to be covered by separate policies.

However, as the PRA noted, express exclusions for cyber-related claims have not yet become standard in the PI market, even as the risk of silent cyber has become more widely known. This has not been helped by the fact that many professional regulators (SRA, ICAEW, RICS etc.) have mandatory minimum terms which prevent insurers' from unilaterally limiting the cover in their policies, not least where one of the primary aims of such policies is to ensure the protection of the consumer of the professional's services.

Some of the cyber-related scenarios where PI policies may provide cover, unless there are applicable exclusions, include:

- Statutory claims for compensation from clients or other third parties under the Data Protection Act 2018/GDPR for personal data breaches following a cyber-attack on the professional's computer system or accidental loss of data;
- "*Friday afternoon frauds*", where criminals trick the professional's staff into sending them client monies via fake emails;
- Phishing attacks leading to loss of first party or third party funds or corporate/personal data;
- A professional using 3rd party software to provide automated advice to clients, but the software becomes corrupted following a cyber-attack or programming error and the advice provided is wrong;
- Ransomware events where the insured is then unable to properly service clients leading to professional negligence claims.

What is happening in relation to silent cyber in Professional Indemnity Insurance?

All PI policies (and new coverholder arrangements) written through Lloyd's incepting from **1 January 2021** need to either expressly include or exclude cyber cover.

The LMA and IUA have been working hard to develop cyber endorsements for their members for PI policies. The IUA's Professional Indemnity Forum created a Cyber Working Group to review the management of cyber risks in the various PI classes of business and draft model endorsements specifically for PI policies.

Given the variety of potential claims against professionals, it is not always easy to draw the line on whether certain claims, which could be said to be cyber-related in one way or another, should be considered PI risks and fall for cover under PI policies, or are not PI risks and should be excluded and passed to the specialist cyber insurance market. For example, if a hacker steals a professional's own money, one would not expect the PI policy to respond to this loss. But what if it were client money? What if the hacker does not steal the client's money directly, but intervenes in the professional/client email chain, tricking the professional into paying away the client's money to the hacker? Should it make a difference if the professional is negligent in its implementation of its cyber-security measures?

Silent Cyber in Professional Indemnity Insurance

The IUA conducted a wide-ranging survey of the PI and cyber markets, including consulting with insurers, brokers and professionals, to obtain the market's views on numerous claims scenarios and whether certain claims should fall for coverage under PI policies or should be excluded. Taking into account these views, the IUA and LMA have developed model endorsements which seek to delineate cover for certain cyber-related events.

The IUA's model endorsement

The IUA have recently published its model endorsement clause "IUA04-017" and an explanatory note[1]. The general approach adopted by the IUA is:

- Claims and losses *directly* caused by a malicious cyber-attack (called a "*Cyber Act*"), system failure (of the system owned or controlled by the Insured or any other party acting on their behalf) or virus transmission are excluded, but those losses *indirectly* caused are potentially covered.
- There is a total exclusion for all claims for breach of Data Protection law (as defined).
- There is also a total exclusion for claims, losses etc *directly* or *indirectly* caused by the failure of service of (a) any ISP, cloud or telecoms supplier, unless that failure is by a supplier hosting the hardware or software owned by the Insured, or (b) a utility service provider where such failure impacts the Insured's computer system;
- Cover otherwise provided for reconstituting lost or damaged documents will not apply to computer data.

Leaving aside for one moment the total exclusion of "Data Protection law" and "data-related loss of document" claims, the IUA endorsement seeks to distinguish cover between: (i) claims caused by third party deliberate "bad actors" and interruption to the hosting of the Insured's hardware and software (claims only excluded if *directly* caused by such perils) and (ii) accidental interruption to the Insured's computer system (claims excluded if *directly* or *indirectly* caused by such perils).

The IUA endorsement language used requires (as is common with any insurance policy) an understanding of the legal concept of "proximate cause" of a loss. In summary, something is the proximate cause if it is the dominant, real, operative or effective cause of loss. The Courts have held that to be "*directly*" caused includes a requirement of proximate cause but "*indirectly*" caused implies a weaker causative connection for a policy exclusion to apply. What that lesser causative requirement is has been debated in past cases[2] and is ultimately an issue of judicial impression based on the facts of any particular case.

The IUA's Explanatory note explains that the intention behind excluding losses caused *directly* but not *indirectly* by specified cyber events is to exclude "pure" cyber losses where there has not been any "*intervening*" act or omission on behalf of the Insured, which should fall to the specialist cyber risks insurance market. The intention is for the PI policy to cover claims where the proximate cause of the loss was the professional firm's act or omission and where the cyber event was more peripherally involved.

The total exclusion of claims for breaches of Data Protection law excludes claims that may well have been previously 'silently' covered by many PI policies. For example, claims for statutory compensation for personal data breaches under the GDPR, where the professional has breached the confidentiality of its clients' personal data as a result of a cyber-attack or accidental loss of data. Cover for these statutory claims are clearly excluded by the IUA endorsement. Depending on the facts, however, such claims may effectively be brought alternatively as claims for breach of contract or tortious claims for negligence, breach of confidentiality or misuse of private information – which may well still be covered by the main PI policy insuring clause.

[1] Available at: https://www.iua.co.uk/IUA_Member/Clauses/eLibrary/Clauses.aspx

[2] See *Crowden v QBE Insurance (Europe) Ltd* [2017] EWHC 2597 (Comm) for a useful overview of the application of such language to policy exclusions

Silent Cyber in Professional Indemnity Insurance

The LMA's model endorsement

The LMA have also just published its model endorsement clause, "LMA 5531". The LMA have taken a slightly different approach to the IUA in their model endorsement:

- There is a total exclusion for all claims and losses *directly* or *indirectly* caused by or contributed to by a malicious cyber-attack (also called a *"Cyber Act*").

- All claims and losses *directly* or *indirectly* caused by a *"Cyber Incident"* are:

    i. Excluded. *Cyber Incident* is defined as (a) any error or omission involving access, processing, or use of or operation of the Insured or any other party's computer system, and (b) a systems failure of the Insured or any other party's computer system; but

    ii. There is a limited "write-back", providing cover for such *Cyber Incidents* if the claim against the Insured arises out of an actual or alleged breach of "Professional Duty" involving access, processing, or use of or operation of the Insured or any other party's computer system or data, unless such breach of Professional Duty by the Insured is caused by, contributed to by, resulting from, arising out of or in connection with a *Cyber Act* (i.e. malicious cyber-attack).

- Like the IUA's endorsement, there is a total exclusion for all claims for breach of Data Protection law (as defined).

Whilst the applicability of the IUA and LMA endorsement will depend upon the specific facts of any case, the exclusion for cyber-related events in the LMA's endorsement is therefore potentially wider than the IUA endorsement, given it totally excludes claims directly or indirectly caused by "Cyber Acts" i.e. malicious cyber-attacks, whereas the IUA endorsement only excludes claims *directly* arising from these types of events.

What about regulated professionals?

For non-regulated professionals, the model endorsements that have been prepared by the LMA and IUA should ensure their members can meet Lloyd's deadline of 1 January 2021 for making it clear that their policies either expressly include or exclude cyber cover.

However, it seems unlikely that policies for all regulated professionals such as solicitors, surveyors and accountants will be ready by 1 January 2021, given the need for the regulated bodies such as the SRA, RICS and ICAEW to approve any changes to their minimum terms to allow any cyber related exclusions. History shows that changes to minimum terms wordings are difficult to agree and, even if ultimately agreed, take time to implement, not least due to the various stakeholders and the desire by the professional bodies for their members and the consumers of their services to benefit from the widest possible cover. It will remain to be seen how Lloyd's (and potentially the PRA) will approach any delays in updating PI policies for regulated professions.

The future

The insurance market has made a lot of headway in dealing with the problem of silent cyber.

Some brokers have complained of a rush to exclusions, some of which are too wide, including some which seemingly exclude *any* loss where technology is involved in the loss in any way. Many insurers will inevitably take a cautious approach against the backdrop of regulatory scrutiny, impending deadlines and gaps in knowledge. Wordings and the understanding of the market will certainly continue to develop. Professionals should carefully consider and seek advice on their cyber risk exposure from their brokers in light of these developments and wording changes to ensure they are sufficiently protected.

It is undoubtedly a positive that there will be more clarity over cyber coverage and policyholders and brokers can negotiate with insurers with greater certainty and look to specialist cyber policies as necessary.

Such focus also feeds into a separate difficult coverage problem which exists in the world of specialist cyber policies. There is very little market consistency in the drafting and language of specialist cyber policy wordings, and a wide range of new cyber policy wordings and

exclusions continue to come to the market. The cover provided by these different cyber policies across first and third party losses is diverse, and some policies have been criticised as providing weak and illusory coverage[3].

With such a variety of untested policy language, and given the ever-increasing cyber risks faced by all types of organisations and the potentially existential losses involved, navigating the cyber policy market is a potential minefield and insureds require expert cyber brokers (and potentially expert cyber lawyers) to understand and ensure they obtain sufficient coverage for their cyber exposure.

On the other hand, cyber policies can provide cover that can prove life-saving to professionals and other businesses should a cyber event occur[4]. The steps to eradicate silent cyber mean that obtaining proper cyber risks cover is more important than ever.

For further information please contact:

Andrew Jones
Senior Associate
+44 (0) 20 7469 0420
ag.jones@beale-law.com

Ahmed Mian
Trainee Solicitor
+44 (0) 20 7469 0423
a.mian@beale-law.com

[3] See Mactavish's "Cyber Risk and Insurance" report, November 2018.

[4] See, for example, our recent article on the SRA's recent review of the costs and consequences to various firms of solicitors following cyber-attacks: here.