Solicitors Regulation Authority

Professional indemnity insurance (PII) - cyber cover:

Consultation

April 2021

Contents

About this consultation

We are consulting on a proposal to make a change to our minimum terms and conditions (MTCs) for the professional indemnity insurance (PII) that we require all the law firms we regulate to have in place.

Our proposal is to add a clause into the MTCs that clearly sets out what is and what is not covered in the event of a firm being subject to a cyber-attack/event. This is in line with the expectations that the Prudential Regulation Authority and Lloyd's of London have of insurers because the risk of cyber-attacks on individuals and businesses has increased.

Our objective is to provide absolute clarity for law firms, insurers, and consumers without altering the scope of consumer protection provided by our PII arrangements.

The consultation is open for your comments from 13 April 2021 until 25 May 2021. After it closes, we will collate and analyse any responses. We will then confirm our final position.

How to respond

Online questionnaire

Our online consultation questionnaire is a convenient, flexible way to respond. You can save a partial response online and complete it later. You can download a copy of your response before you submit it.

Start your online response now. https://form.sra.org.uk/s3/pii-cyber

Reasonable adjustment requests and questions

We offer reasonable adjustments. Read our policy to find out more.

Contact us at piicyber@sra.org.uk if you need to respond to this consultation using a different format or if you have any questions about the consultation.

Publishing responses

We will publish and attribute your response unless you request otherwise.

Background to consultation

1. Over the years, the risk of cyber-attacks on individuals and businesses has increased and, year on year, the size and scale of these attacks are changing. Law firms are exposed to cyber risks because, for example, they hold and transfer large sums of money and sensitive corporate and personal data.

2. We and other regulators have responded, providing a range of resources to support firms to address the risks.[1] If a firm's clients do suffer loss through a cyber-attack, the firm is likely to make a claim on its PII policy.

3. The Prudential Regulation Authority (PRA) which regulates and supervises a range of financial firms including insurers, expects insurers to be able to identify and manage the cyber insurance risk. Lloyd's of London (Lloyd's), which runs one of the major insurance markets, is concerned that some insurance policies, are not specific enough about exactly what cyber-related losses are, and are not, covered.

4. This means that firms might wrongly think they have PII cover for certain types of loss arising out of a cyber-attack, or that firms might be paying for the same cover through several policies (for example, the separate cyber insurance policies) when they have no need to do so.

5. The PRA and Lloyds are therefore requiring insurers to take steps which includes making provision for cyber losses explicit in their insurance policies, including for PII. The detail of their requirements can be found in **Annex one**.

Our proposal

6. PII policies for law firms are written on a broad 'civil liability' basis[2] for claims arising out of its 'private legal practice'. This makes sure that there is protection for consumers for claims arising from legal work, regardless of the nature of the event which has resulted in the loss.

7. Given the PRA and Lloyds expectations, we are consulting on adding a clause to the MTCs that makes it explicit that the consumer protection under our PII arrangements equally applies if the loss is because of a cyber-attack/event.

8. This aims to:

    a. maintain the current level of consumer protection intended by our insurance arrangements

[1] https://www.sra.org.uk/solicitors/resources/cybercrime/

[2] A civil liability policy does not set boundaries (other than the exclusions) as to the nature of the wrongdoing. It can include more than just negligent acts errors or omissions and include breach of duty of trust, conflicts of interest, breach of client money rules. These claims may not necessarily arise from negligence but will be covered.

b. allow insurers to be clear and therefore better able to manage their exposure

c. provide clarity to law firms about what is and is not covered by their PII policy so that they are in better position to review the benefit of purchasing a cyber policy for other risks, for example to the firm itself.

9. The proposed change is to clarify that losses caused by a cyber-attack which fall within scope of a claim for civil liability against a regulated law firm must be covered. This means that for example, any redress to a client of the firm or an aggrieved third party would be covered, in line with the consumer protection offered by PII. To date, we have not been called to arbitrate on a dispute between law firms, consumers, and insurers about whether our existing MTCs cover consumer losses caused by a cyber-attack.

10. Also, our view is that the proposed change should not directly alter the premiums paid by law firms as claims for civil liability caused by a cyber-attack have always been considered to be in scope of a MTC compliant PII policy and reflected in any premium that a law firm pays.

11. The loss to the business itself – the law firm - caused by the cyber-attack (first-party losses) would not be covered, as is currently the case. The PII policy is not intended to provide cover for first-party losses suffered by the law firm including those caused by a cyber-attack, for example, loss of the firm's own money or the costs of rectifying any reputational issues.

12. Our MTCs already set out that the PII cover is excluded from indemnifying for example, trading debts or liabilities, public (injury/death) liability and partnership or employment disputes. So for example, a fine from the Information Commissioner's Office as a result of a cyber-attack affecting the firm's operations would not be expected to be covered by the PII policy. Many firms choose to purchase additional insurance products to cover any business losses caused by events of this nature and our proposal does not affect those insurance products.

Our approach

13. The way we have approached the change to the MTCs is to:

a. add an exclusion which sets out that the insurance may exclude liability of the insurer to indemnify a law firm in respect of, for example, first-party losses caused by a cyber act or a partial or total failure of any computer system

b. make absolutely clear that any such exclusion should not exclude or limit any liability of the insurer to indemnify a law firm against any claim for civil liability. This includes the obligation to remedy a breach of the SRA Accounts Rules. So for example, a cyber-attack which affects the law firm's own IT systems that results in a claim for civil liability from a client or third party would be covered.

14. The changes are not intended to affect current protections where for example, a law firm's laptop containing personal client data is left on a train by an employed solicitor travelling to or from a meeting, and the data is accessed by a third party which results in a loss to the client. This type of scenario is covered by the scope of a PII policy and would not change as a result of the proposals in this consultation.

15. We are aware that the International Underwriters Association (IUA) has published an endorsement/clause specifically for PII policies that it considers would provide affirmative cover for cyber risks. Our view is that this endorsement/clause - which we know some insurers and Lloyd's syndicates have accepted as a model clause - does not reflect the scope of cover for consumers as set out in our PII arrangements. One of the risks that our proposal manages is that that some insurers/Lloyd's syndicates may seek to add the IUA clause into their PII polices. The IUA clause reduces consumer protection, so that for example, a loss of client money caused by a cyber-attack might not be covered. The IUA clause would not therefore be appropriate and we are not proposing to adopt it, but it has some helpful definitions that we have adapted for the purposes of our draft clause.

16. The draft amendments to the MTCs and an explanatory note is attached at **Annex two**. This consultation is to seek views on the drafting and to be sure that the changes do not inadvertently reduce or expand the scope of cover provided by PII arrangements. The changes are not intended to do that.

Impact on law firms and consumers

17. We have considered whether our proposed changes might have a negative impact on:

    - vulnerable consumers of legal services, and
    - particular groups of solicitors or firms.

18. We have not identified any negative impacts as we have worked to develop our proposed changes to the MTCs in respect of claims arising from a cyber-attack.

19. The proposed course of action:

    - maintains the current protection for all consumers
    - provides clarity for insurers, law firms and consumers to help reduce the risk of any disputes about coverage arising, and
    - should not directly alter the premiums paid by law firms.

20. Insurers can continue to offer standalone cyber insurance policies to law firms which provide cover for first-party (the law firm) losses for example, loss of the firm's own money or the costs of rectifying any reputational issues. We are not however, mandating that law firms must buy separate cyber insurance policies in the same way that we do not mandate that a firm must have for example, employer liability insurance or business interruption insurance.

Our questions

21. We would like to hear what you think about our approach to changing the MTCs. If you believe we should be considering a different approach, please tell us what this could be. We would also welcome any information you might have about the potential impacts of our approach.

    Question 1: Do you agree with the proposed change to our MTCs?

    Question 2: Does the draft clause, in your view, maintain, expand or reduce the current scope of consumer protection afforded through our PII arrangements?

    Question 3: Does the draft clause bring about any unintended consequences and if yes, how might the draft clause be amended?

    Question 4: Are there any other impacts which you think we need to consider?

Next steps

22. Following this consultation, we will review all responses to the consultation and confirm our final position. We will then proceed with our application to the Legal Services Board (LSB) with a view to changes being made in time for 1 October 2021, or earlier if possible.

23. In the interim, insurers should not be altering the terms of their (SRA) PII policies. We do not expect insurers to be using the proposals or any lack of specificity to imply that firms are not covered for claims in respect of civil liability, or other losses in scope of the MTCs, that arise because of a cyber-attack.

24. As mentioned above, insurers can continue to offer standalone cyber insurance policies to law firms which provide first-party cover. This is a decision for the firm to consider having regard to its own risk profile and how it runs its business.

Annex one: What have the PRA and Lloyd's required of insurers?

1. The PRA in its July 2017 supervisory statement identified certain actions that insurers could follow up to manage this risk[3]. These actions included for example, explicitly confirming cover, and adjusting the premium to reflect this or introducing robust wording that sets out what risks are excluded. This would enable insurers to make adequate capital provisions linked to the risk, which is the PRA's main desired outcome.

2. In January 2019, the PRA followed this up with the CEOs of insurers and made clear its expectation that all insurers should have action plans for discussion[4] to reduce the unintended exposure which can be caused by non-affirmative (silent) cyber cover[5]. The PRA set out its expectations of insurers on the prudent management of cyber underwriting risk in three broad areas:

    - actively managing non-affirmative ('silent') cyber risk
    - setting clearly defined cyber strategies and risk appetites that are agreed, and
    - building and continuously developing insurers' cyber expertise.

3. The PRA identified that PII policies were particularly likely to be exposed to various degrees of silent cyber risk. This was because of the way professional services businesses (including law firms) transact with clients and third parties. They are exposed to cyber risks because for example, because they hold and transfer large sums of money and sensitive corporate and personal data.

4. Lloyd's followed with its own review, which went further, by mandating that all policies of its syndicate members had to provide clarity regarding cyber coverage by either expressly excluding or expressly providing affirmative cyber cover[6]. Lloyd's said that this approach particularly focused on driving the eradication of silent cyber risk from traditional lines of insurance by encouraging insurers to identify the exposure and either clearly exclude or affirmatively include cover in policies. In January 2020, Lloyd's stated that it expected its members to make the necessary changes by 1 January 2021.

[3] https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/supervisory-statement/2017/ss417.pdf?la=en&hash=6F09201D54FFE5D90F3F68C0BF19C368E251AD93
[4] https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/letter/2019/cyber-underwriting-risk-follow-up-survey-results
[5] Non-affirmative cyber, also known as silent cyber, refers to potential cyber exposures contained within insurance policies which may not implicitly include or exclude cyber risk
[6] https://www.lloyds.com/~/media/files/the-market/communications/market-bulletins/2019/07/y5258.pdf

Annex two: Proposed draft changes to the MTCs

6. Exclusions

The insurance must not exclude or limit the liability of the *insurer* except to the extent that any *claim* or related *defence costs* arise from the matters set out in this clause 6.

…

6.[ ] Cyber, infrastructure and Data Protection Law

The insurance may exclude, by way of an exclusion or endorsement, the liability of the *insurer* to indemnify any *insured* in respect of, or in any way in connection with:

(a) a *cyber act*
(b) a partial or total failure of any *computer system*
(c) the receipt or transmission of malware, malicious code or similar by the *insured* or any other party acting on behalf of the *insured*
(d) the failure or interruption of services relating to *core infrastructure*
(e) a breach of Data Protection Law

provided that any such exclusion or endorsement does not exclude or limit any liability of the *insurer* to indemnify any *insured* against:

(i) civil liability referred to in clause 1.1 (including the obligation to remedy a breach of the SRA Accounts Rules as described in the definition of *claim)*
(ii) *defence costs* referred to in clause 1.2
(iii) any award by a regulatory authority referred to in clause 1.4.

In addition, any such exclusion or endorsement should not exclude or limit any liability of the *insurer* to indemnify any *insured* against matters referred to at (i), (ii) and (iii) above in circumstances where automated technology has been utilised.

Additional Defined Terms to add to the glossary:

1. *Cyber Act* means an unauthorised, malicious or criminal act or series of related unauthorised, malicious or criminal acts, regardless of time and place, or the threat or hoax thereof, involving access to, processing of, use of or operation of any *Computer System*.

2. *Computer System* means any computer, hardware, software, communications system, electronic device (including, but not limited to, smart phone, laptop, tablet, wearable device), server, cloud or microcontroller including any similar system or any configuration of the aforementioned and including any associated input, output, data storage device, networking equipment or back up facility.

3. *Core infrastructure* means any service provided to the *insured* or any other party acting on behalf of the *insured* provided by an internet services provider, telecommunications provider, or cloud provider.

4. *Data Protection Law* means any applicable data protection and privacy legislation or regulations in any country, province, state, territory or jurisdiction which govern the use, confidentiality, integrity, security and protection of personal data or any guidance or codes of practice relating to personal data issued by any data protection regulator or authority from time to time (all as amended, updated or re-enacted from time to time).

Explanatory Note (not forming part of the SRA Standards & Regulations)

1. The title of this clause is a stylistic proposal to explain what types of loss the clause discusses.

2. The definition of cyber act aligns with the definition in the International Underwriting Association's (IUA) model clause and is considered appropriate for the MTCs.

3. The definition of computer system aligns with the definition in the IUA model clause and is considered appropriate for the MTCs.

4. Core infrastructure is a proposed new definition within the MTCs, which utilises some language from the IUA model clause, but does depart in other aspects.

5. Our interpretation of the IUA model clause is that it 'writes back in' some (first party and third party) losses where the insured's own hardware/software/computer system experiences an issue. That might be appropriate for other PI policies, but is not necessary to state in the MTCs. The only type of loss intended to be covered by the MTCs is loss flowing from an issue with the insured's own systems where civil liability also occurs. This is clarified in the draft cyber clause for the MTCs in the paragraph beginning: 'provided that any such exclusion or endorsement…'

6. The definition of data protection law follows the definition in the IUA model clause and is considered appropriate for the MTCs. The Royal Institute for Chartered Surveyors for example, has consulted on language that refers to the GDPR and subsequent legislation enacted in the UK. We do not think is it strictly necessary to add this distinction as titles might change.

7. The last paragraph of the proposed additional clause beginning 'In addition, any such exclusion…' is designed to confirm the position in relation to events where third-party losses arise following the use of technology in the provision of advice. Examples could include Stamp Duty Land Tax calculators or auto-generated advice. We consider that, in circumstances, where technology is utilised to provide advice that results in loss covered by the civil liability clause within the MTCs, then such losses should be covered by the PII policy.

8. 'Automated technology' is purposefully not drafted as a new defined term, given the likelihood that technological processes such as chatbots and AI will develop over time. Absent a specific definition, parties (and ultimately a court) would look to use the ordinary meaning/dictionary definition of policy language when interpreting that phrase. We consider that 'automated processes' sufficiently covers use of the technologies currently in purview and allows for future development in this sphere.