

Consultation: Changes to Professional Indemnity Insurance (PII) – cyber cover.

We welcome responses from our regulated entities, insurance companies, organisations which represent the interests of consumers and other stakeholders including members of our regulated community, other frontline regulators, and other interested parties.

CONTENTS PAGE

	Page
Executive Summary	3
Background to the proposal	4
Our proposal	4
Our approach	5
Implications for consumers	5
Implications for firms	6
Required rules changes	6
Summary of questions and how to respond	6

Annex 1: Amendments to the Professional Indemnity Insurance Minimum Wording

EXECUTIVE SUMMARY

Introduction

CILEx Regulation Limited (CRL) is the independent regulator for Chartered Legal Executives, other grades of CILEX membership, CILEX Practitioners and firms. We take a risk-based and outcomes-focused approach to regulation, by working constructively with our regulated community to ensure that they deliver the best outcomes for clients. We have set clear principles within our Code of Conduct and inform the public of the standards they can expect. We believe this provides a balanced approach.

What are we proposing?

This consultation seeks views on CRL's proposal to clarify the scope of Professional Indemnity Insurance (PII) cover when a law firm has been subject to a cyber-attack/computer breach.

Why are we proposing this change?

This proposed change is in response to the Prudential Regulation Authority (PRSA) and Lloyds of London introducing a requirement for to make provision for cyber losses explicit in their insurance policies.

When will the changes come into effect?

These proposed changes are planned to come into effect immediately after the rules changes outlined in the consultation have been approved by the Legal Services Board.

What are the implications to consumers of the change?

The changes have been designed to ensure that existing consumer protections are maintained.

What rules changes are we proposing?

CRL is proposing to make changes to the following rules:

- Professional Indemnity Insurance Minimum Wording (**Annex 1**)

The rules are annexed to this consultation document and the amendments are set out in tracked changes.

BACKGROUND TO THE PROPOSAL

1. The risk of cyber-attacks on individuals and businesses has continued to increase and, because of the large sums of money and sensitive data that law firms hold, they have become more regularly exposed to cyber risks. If a firm's clients do suffer loss through a cyber-attack, the firm is likely to make a claim on its PII policy.
2. The Prudential Regulation Authority (PRA) which regulates and supervises insurance providers, now expects insurers to be able to identify and manage their exposure to 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 sufficiently specific enough to be able to identify which cyber-related losses are covered and which are not covered.
3. The PRA and Lloyd's now require insurers to make provision for cyber losses explicit within their insurance policies, including policies for PII. This will mean that, in future, firms have clarity on which of the types of loss arising out of a cyber-attack will be covered, and that firms will have the appropriate cover in place to enable them to manage risks (through for example a cyber insurance policy).
4. CRL is consulting to bring its minimum wording into line with the protections provided by other regulators' minimum terms and conditions and to provide clarity on the scope of PII cover available when a law firm has been subject to a cyber-attack/computer breach.

OUR PROPOSAL

5. PII policies for law firms are written on a broad 'civil liability' basis 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.
6. CRL is consulting on adding a clause to the Minimum Wording that makes it explicit that the consumer protection under its PII arrangements equally applies if the loss is because of a cyber-attack/computer breach.
7. By the addition of this clause, CRL's intention is to:
 - a. maintain the current level of consumer protection intended by its insurance arrangements
 - b. allow insurers to be clear and therefore able to manage better their exposure
 - c. provide clarity to law firms about what is and is not covered by their PII policy so that they can better assess the benefits of purchasing a separate cyber insurance policy.
8. In line with other regulators' requirements, CRL is proposing 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. 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.

9. CRL believes 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 within scope of a compliant PII policy and, therefore, reflected in any premium that a law firm pays.
10. This would maintain the current position, whereby any loss to the law firm itself caused by the cyber-attack would not be covered. CRL agrees that the PII policy is not intended to provide cover for cyber-attack losses suffered by the law firm, such as loss of its own money, the costs of rectifying any reputational issues, or indemnifying, for example, trading debts or liabilities, public (injury/death) liability and partnership or employment disputes.
11. CRL does not believe that this change will impact upon firms seeking to purchase additional insurance products to cover any business losses.

OUR APPROACH

12. The changes that CRL is proposing to its Minimum Wording is in line with that adopted by other regulators and is based on two key additions to the wording.
13. Firstly, the addition of an exclusion setting out that the insurance may exclude liability of the insurer to indemnify a law firm in respect of their own losses caused by a cyber act or a partial or total failure of any computer system.
14. Secondly, by providing clarity 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. 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.
15. In line with other regulators CRL has decided not to adopt the endorsement/clause published by the International Underwriters Association (IUA) specifically for PII policies that the IUA considers would provide affirmative cover for cyber risks, because it does not reflect the scope of cover for consumers as set out in our PII arrangements.
16. This consultation seeks views on the drafting of the changes to the Minimum Wording and to be sure that the changes do not inadvertently reduce or expand the scope of cover provided by CRL's PII arrangements. The proposed changes are not intended to have this effect.

IMPLICATIONS FOR CONSUMERS

17. In putting forward these changes, CRL has considered whether the proposal has a negative impact on consumers of legal services, in particular those that may be considered as vulnerable consumers.
18. CRL believes that the changes will:

- a. maintain the current protection for all consumers, and
- b. will assist in reducing the possibility of future disputes by providing clarity on coverage.

IMPLICATIONS FOR FIRMS

19. CRL has considered whether the proposal may have a negative impact on CILEX Authorised Entities and has not identified any such impacts in respect of claims arising from a cyber-attack.
20. The proposed course of action provides clarity for both insurers and law firms on scope of coverage and CRL is hopeful that the change should not alter the premiums to be paid by law firms.
21. Whilst CRL is not mandating that a law firm must have in place a separate cyber insurance policy, CRL recognises the benefits that standalone cyber insurance policies provide for law firms by providing protection against the loss of the firm's own money, or the costs of rectifying any reputational issues.

REQUIRED RULE CHANGE

22. To introduce the changes outlined in the consultation, CRL is proposing to amend its Professional Indemnity Insurance Minimum Wording
23. These changes are set out in annex 1.

SUMMARY OF QUESTIONS AND HOW TO RESPOND TO THE CONSULTATION

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

Question 2: Does the draft clause affect the current scope of consumer protection afforded through our PII arrangements?

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

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

Please give reasons for your answers.

How to respond

Please send your response to CILEx Regulation by email to consultations@cilexregulation.org.uk. Please mark it for the attention of David Pope.

Submission deadline

Please respond by **5pm on 22 June 2022**.

Annex one: Proposed draft changes to the Minimum Wording

4. Exclusions

4.14 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
- (ii) defence costs referred to in clause 1.4 that would have been covered under the insurance even absent an event at 4.14 (a) to 4.14 (e) detailed above

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), and (ii) above in circumstances where automated technology has been utilised.

Additional Defined Terms to add to 7. Interpretation and Definitions:

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).