THE FACULTY OFFICE

Professional Indemnity Insurance – Cyber cover

This is one of two issues to do with professional indemnity cover which the Advisory Board are asked to consider at its December meeting (the other relates to cover for work intended for the US & Canada and is covered in a separate paper).

It is clear that the risk of cyber-attacks on individuals and businesses has increased and, year on year, the size and scale of these attacks has changed. What is less clear is the extent to which a Professional Indemnity Insurance (PII) Policy provides cover in the event of a cyber-attack/event. Law firms and individual notaries are exposed to cyber risks because, for example, they hold and transfer large sums of money (especially those undertaking conveyancing and probate/estate administration) and sensitive corporate and personal data. If a Notary's clients do suffer loss through a cyber-attack, the Notary is likely to have to make a claim on their PII Policy.

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.

This means that firms or individual notaries might wrongly think they have PII cover for certain types of loss arising out of a cyber-attack, or that they 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.

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 (ie what is and is not covered).

As a result of this, the Solicitors Regulation Authority (SRA) consulted in the Summer on proposals to amend its Minimum Terms and Conditions (MTCs) with the intention of providing clarity and to ensure that consumers are protected:

> *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, (the SRA) 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*
>
> *Also, our (the SRA's) 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.*

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.

A copy of the relevant amended MTCs is set out in the Annex. Assuming these changes are approved by the LSB, it will be clear that any notary who operates their practice through the SRA regulated law firm in which they are a partner, member, director or employee will have clarity of cover as the MTCs also include cover where an insured or an employee of an insured is acting "*as a personal representative, trustee, attorney, **notary**, insolvency practitioner or in any other role in conjunction with a practice".* An employee includes: *"without limitation, a solicitor, lawyer, trainee solicitor or trainee lawyer, consultant, associate, locum tenens, agent, appointed person, office or clerical staff member or otherwise" (and including a secondee from outside and/or employee seconded to work elsewhere).*

The Faculty Office has not, to date, sought to impose a set of minimum terms and conditions for PII cover for notaries who take out their own policy save in respect of the minimum sum insured (currently £1m). Claims against Notaries are few (particularly those undertaking solely notarial activities) and this risk is reflected in the level of premium and excess payable for the majority of stand alone PII policies as compared to equivalent solicitor firm cover. However, with increasing numbers of notaries now opting to obtain separate cover, to ensure that consumers (clients) are adequately protected in accordance with the Regulatory Objectives[1], it may be that a set of MTCs of our own, similar to but not exceeding those of the SRA may become necessary.

One reason why our own MTCs might become necessary is 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 (ie clarity of cover). This endorsement/clause - which 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 the SRA's proposed PII arrangements. The IUA clause reduces consumer protection, so that for example, a loss of client money caused by a cyber-attack might not be covered which would leave consumers and notaries exposed.

As regard the issue at hand, the Advisory Board are asked to consider, given the current nature of notarial activities and the extent to which that work is changing/likely to change, whether the threat or risk of cyber-attack is currently, or might become, significant and how this might be best addressed in the short to medium term.

The Faculty Office
1 December 2021

[1] Legal Services Act 2007 1(1)(d) protecting and promoting the interests of consumers

Annex

Clarificatory changes to the SRA Minimum Terms and Conditions (MTCs) of Professional Indemnity Insurance (Annex 1 to the SRA Indemnity Insurance Rules)

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 inured 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 that would have been covered under the insurance even absent an event at 6(a) to 6(e) detailed above

(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.

Amendment to current Defined Terms

Defence costs

means legal costs and disbursements and investigative and related expenses reasonably and

necessarily incurred with the consent of the insurer in:

a. defending any proceedings relating to a claim; or

b. conducting any proceedings for indemnity, contribution or recovery relating to

a claim; or

c. investigating, reducing, avoiding or compromising any actual or potential claim;

or

d. acting for any insured in connection with any investigation, inquiry or disciplinary proceeding (save in respect of any disciplinary proceeding under the authority of the SRA or the Tribunal), and does not include any internal or overhead expenses of the insured firm or the insurer or the cost of any insured's time.

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 ComputerSystem.

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 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).