27 November 2020

Professional Indemnity Cyber Endorsement - Explanatory Note[1]

Introduction

In late 2019, the IUA's Professional Indemnity Forum (PIF) created a working group of committee members to consider how cyber risks are treated in the professional indemnity (PI) market and the degree of overlap or gaps in respect of traditional, standalone cyber insurance products. The key driver for this initiative is the ongoing regulatory scrutiny by the Prudential Regulation Authority (PRA) into cyber risks provided in the non-standalone cyber market and their requirement that insurers suitably identify, assess and manage their cyber liabilities. Underpinning these principles are reservations that insurers in non-standalone cyber classes of business are not affirmative in their policy approach to cyber risks and also do not always sufficiently consider the potential for systemic cyber exposures, thus leading to potential coverage and wider prudential issues.

The PRA's work, and also the growing size and sophistication of the standalone cyber market and scope of cyber risk, has led to a re-evaluation of cyber risks in most non-standalone markets. As a reaction to this, Lloyd's published a Market Bulletin requiring Managing Agents to be express in their policy approach to cyber risks (Y5258 in July 2019) and follow up correspondence (Y5277 in January 2020) identified that professional indemnity risks should have 'compliant' policy provisions in place by 1 January 2021.

PIF Cyber Working Group

Against this backdrop, the PIF Cyber Working Group (which was extended to include a number of cyber practitioners and a leading law firm) met to discuss the common issues arising in respect of managing cyber risks in the various professional indemnity classes of business and to consider whether a model policy provision could be drafted for use in the PI market which helps meet regulatory expectations.

As a first step, the Working Group agreed that it would be beneficial to survey both the PI and cyber markets to request feedback on some of the 'grey' coverage areas and for views on where claims should ultimately lie. A number of scenarios were developed to facilitate this.

[1] This note is not intended to be exhaustive or definitive and is subject to any views or interpretation by a Court, regulator or similar body. By including this note, the IUA is not providing legal advice and does not accept any responsibility for subsequent interpretation of the commentary or the accompanying model endorsement, or any part thereof. Any party considering adopting any of the model endorsement, or any part thereof, should seek their own legal advice for clarification of the use and intention of the model endorsement.

Responses were provided by 74 practitioners. These consisted of PI and cyber underwriting and claims practitioners, some ancillary class providers (e.g. commercial crime and liability), reinsurers, brokers and a number of law firms. We amalgamated and desensitised the results and engaged with DAC Beachcroft LLP (principally Julian Miller, Partner) to assist in drafting a model endorsement that reflected the results as broadly as possible, cognisant of the PRA and Lloyd's requirements. This latter engagement was not only done for drafting expertise and to stress test the various scenarios but also in recognising that any model provision would need to be discussed with the professional bodies (such as SRA, RICS and the ICAEW) in considering the approach to cyber risks in their respective minimum terms wordings. This latter point obviously only relates to UK PI, though we would emphasise that the endorsement has been drafted in such a way that it would equally apply to insureds located elsewhere.

The Model Endorsement [2]

The model endorsement starts from the principle of ensuring that traditional PI exposures remain covered whilst claims more appropriately covered elsewhere are excluded (most commonly these would fall under a the standalone cyber policy) and where possible following the results of the market survey. Annex 2 provides an overview analysis of all the scenarios within our survey and we will refer to some of the particular scenarios in more detail below. The definitions were developed based on a review of existing model market clauses and legal advice.

Paragraph 1 – for clarity purposes, this paragraph confirms that the provisions in this cyber endorsement overrides other policy provisions in the event that there is competing policy language (though subject to the language in Paragraph 2). As the endorsement only relates to cyber, it is worth noting that any provisions wholly unrelated to cyber risks should not be overridden.

Paragraph 2 – this affirmation language was developed to aid contract clarity and also with the Lloyd's requirements for its' Managing Agents to expressly affirm or exclude cover in mind. It affirms that, unless otherwise stated in this endorsement or by other restrictions in the policy relating to the use of a Computer System, where the policy would otherwise respond there will no restrictions on recovery solely due to use of a Computer System. So, subject to the endorsement provisions, where an otherwise valid, payable PI claim is brought, this will not be limited by the fact that Computer System was incidentally used to complete the professional work. We would stress that Paragraph 2 does not in any way infer that any other cover in the underlying policy is expanded.

Paragraph 3 – this excludes cover for any losses and costs directly caused by, directly resulting from, or directly arising out of, a Cyber Act (which is defined), a partial or total failure of any

[2] The endorsement is an optional tool for practitioners to use as they individually see fit and has been drafted in compliance with all applicable competition laws and processes that IUA applies to all projects of this nature.

Computer System (defined) or virus transmission. It is important to note the definition of Cyber Act only relates to unauthorised, criminal or malicious access to, operation of or use of Computer Systems and that both a) and b) are limited to Computer Systems owned or controlled by the Insured or any other party acting on behalf of the insured. The decision to limit this exclusion to "direct" losses was taken to ensure the endorsement best reflected our survey results; the intention when drafting was that a direct loss would mean there was no intervening act or opportunity for an intervening act (for example, a manual check of work) between the cyber event and the loss. Any loss indirectly caused by, resulting from or arising out of a Cyber Act would not be excluded by this paragraph. It is also worth highlighting that losses excluded would include loss mitigation costs, though only within the strict confines of a Cyber Act.

Paragraph 4 – this excludes cover for any losses and costs arising from any failure or interruption of services relating to core infrastructure and utility providers. The exclusion has been drafted narrowly to exclude (in paragraph 4(a)) the failure of services provided to the insurer (or those acting on their behalf) in respect of internet services, telecommunications and cloud computing. This does not include the hosting of hardware and software owned by the insured. Paragraph 4(b) excludes failures of services provided by utility companies, but only where the failure impacts a Computer System owned by the insured (or those acting on their behalf).

One important difference with paragraph 3 is that this exclusion has a 'direct or indirect' trigger. This reflects the targeted nature of the exclusion, designed to exclude cover for systemic, non-PI risks these services apply to. We did not survey members directly on an infrastructure exclusion but believe that the approach taken fits broadly with the overall intent to provide cover for PI related exposures and not wider system failure, particular of the potentially systemic nature envisaged in the services noted in the paragraph.

Paragraph 5 – breaches of data protection legislation (defined) are subject to a standalone exclusion. These are separated from paragraph 3 because the intention is that paragraph 3 addresses the cause of loss but paragraph 5 addresses the cause of action. It is not the intention that claims in tort or contract are captured under paragraph 5 (see scenario 6.2 below for how this works in practice). In most circumstances, claimed amounts where the cause of action is for breaches of such legislation should be covered by a standalone cyber policy. One caveat to the exclusion is that it applies only to breaches of legislation by the insured or any other party acting on their behalf.

Paragraph 6 - this confirms that cover otherwise provided for reconstituting or recovering lost or damaged documents owned or controlled by the insured on any party acting on their behalf shall not apply to Data (which is defined). In the Data context, these costs are generally picked up in the cyber insurance market. In the non-data (i.e. paper) environment – architects paper records for example – this would remain covered, if provided for in the underlying policy.

Definitions - as noted above, we have tried to mirror the definitions used in the endorsement to those commonly seen in other cyber clauses in the market, albeit not necessarily in the PI market. The intention is that this supports contract clarity and interpretation.

PII Coverage Scenarios – General Comments

Most of the scenarios in the survey received largely unambiguous responses, whether from PI or non-PI markets. Consequently, the majority of the scenario results could be straightforwardly replicated in the endorsement. However, there were some areas where practitioner views were mixed. This was in some part, we think, due to differing interpretations of the scenarios, which was further evidenced by some of the comments we received in addition to the basic risk allocation answer. However, it is also reflective of the fact that there are undoubtedly areas that require careful underwriting consideration. We expand on these in more detail below. Where the survey results were largely undecided in terms of where the coverage should be written we have made a judgement call on the default coverage position and explained our rationale below. The model endorsement can, of course, be amended if users wish to alter the scope of cover.

Specific Scenarios - Commentary

Scenario 1.3 - Theft via Cyber Hacking (hacker changes details, leads to wrong payment) (1st Party)

Our interpretation when drafting is that this loss is an indirect result of the hack (the intervening step being the negligent sending of funds by the insured) so the exclusion in paragraph 3 of the endorsement is not invoked. This differs from the scenario where a hacker steals the funds directly (1.1 of our survey) where there is no intervening step), which would trigger paragraph 3 of the endorsement. In both instances, however, these are first party losses which are normally not covered under a PI policy. Consequently, (in the absence of a first party loss extension in the policy) we would not expect there to be cover in this scenario.

Scenario 1.4 - Theft via Cyber Hacking (Hacker Changes Details) (3rd Party)

The underlying analysis is the same as 1.3 above and we would not expect the endorsement to exclude this type of loss. As this is a third party loss, PI policies may therefore respond depending on the policy terms and conditions. The same differentiation is true for 1.1 vs 1.2.

Scenario 1.6 - IP Theft via Cyber Hacking – theft of the IP of the Insured's client (3rd Party)

This was one of the scenarios where respondents were mixed on whether the PI policy should respond. The default approach adopted is that this claim would be excluded by the Cyber Act exclusion, which covers malicious and criminal acts. This aligns with Scenario 1.1, the only difference between what is stolen (money instead of IP).

Scenario 2.1 - Mandate Fraud (Social Engineering) (1st Party)

This analysis broadly follows Scenario 1.3 above. Although we expect social engineering to be captured as a malicious or criminal act, the transfer of the funds by the insured is an intervening step making this an indirect loss (by our interpretation). Paragraph 3 of the endorsement would therefore not be invoked but as per Scenario 1.3 above, first party losses would not be covered unless provided for in the underlying policy.

Scenario 2.2 - Mandate Fraud (Social Engineering) (3rd Party)

As per Scenario 2.1, although social engineering is likely captured as a malicious or criminal act, this is likely an indirect loss with the transfer of the funds being the intervening step. Consequently, the exclusionary language in paragraph 3 would not be invoked and cover provided subject to the underlying policy – this is in line with the majority view of survey respondents.

Scenario 2.3 - CEO Fraud (Phishing) (1st Party)

The analysis of this scenario is as Scenario 2.1 above.

Scenario 2.4 - CEO Fraud (Phishing) (3rd Party)

The analysis of this scenario is as Scenario 2.2 above.

Scenario 3.1 - Malware Spreading to Clients

This is intended to be excluded (following the survey results) under paragraph 3(c), which excludes 'the receipt or transmission of malware, malicious code or similar'. This analysis applies equally to Scenario 4.1 (virus spreading to clients where the insured is a professional marketer).

Scenario 4.2 - Hacker Posts Libellous Comments on Client Account (Insured is a Social Media Agency)

This was the most contentious scenario with 51% of respondents believing that this is a PI risk. On reflection, we felt that this type of cover would likely not be needed by most professions (the scenario being specific to a social media agency) and that this exposure may be covered by media liability cover in a cyber policy. As such, it was agreed that the default would be that cover would not be provided but in the knowledge that individual risks may necessitate an amendment to the endorsement.

Scenario 5.2 - Liability for Client Loss from Failure to Give Advice (due to Ransomware Event)

The failure to provide advice would be an intervening step, so this is an indirect result of a Cyber Act and therefore not excluded.

Scenario 6.2 - Accidental Email of Confidential Data to Incorrect Third Party

Whilst claims brought under Data Protection Law would be excluded by paragraph 5 of the endorsement, any third party claims brought in tort, or for breach of contract (i.e. the material exposure for a PI risk), are not excluded by this endorsement. Consequently, the policy would, subject to its terms and conditions, respond accordingly.

Scenario 7.1 - Professional Error due to Corrupt Professional Software

The provision of professional advice is the intervening step following the corrupt software and is the basis for the PI claim. We would therefore expect that, in the majority of circumstances, this would be covered. Our use of 'majority' here reflects that there may be fact-specific arguments where the professional advice was generated automatically or where the error was undetectable to a competent professional. In respect of firms providing automatically generated advice, it may be necessary to amend the endorsement to make clear that the PI would respond.

Scenario 8.1 - Professional advice causes breach of GDPR (insured's client's data was stolen)

Paragraph 5 would not apply because there has not been a breach of Data Protection Law by the insured or any party acting on their behalf, rather the provision of professional advice is the direct cause of the loss. Nor does the loss fall within any of the exclusion triggers within paragraph 3. Consequently, paragraph 2 of the endorsement would apply and the policy, subject to its terms and conditions, would respond to the professional liability claim.

Scenario 8.2.1 – 3rd party financial losses from breach of suitable systems (no insured negligence)

It is worth reiterating the particular facts of this scenario; namely:

"An insured suffers a malicious attack on their systems, which causes a potential breach of the GDPR and subsequent investigation. There has been no negligence on the part of the insured and their IT systems were suitable for their profile and the type of data they hold. Where should compensation payments to 3rd party clients imposed by the ICO, even where there has been no financial loss to the client be covered?"

The scenario relates to ICO imposed compensation payments and paragraph 5 excludes any loss arising out of a breach of Data Protection Law. To this extent, the endorsement follows the survey results of finding that the PI policy should not respond. If the same incident were to cause a third party loss and a claim was brought as either a breach of contract or in tort, rather than a breach of Data Protection Law, the endorsement would not exclude this loss.

Scenarios 8.3.1 to 8.3.4 – GDPR – insured has unsuitable systems

Scenarios 8.3.1, 8.3.2, 8.3.3 and 8.3.4 all deal with GDPR related losses where the insured has inadequate systems in place. Scenario 8.3.1 was considered a PI risk by a small majority (57%)

of respondents, whilst they were also strongly of the view that the other scenarios (as well as 8.2.2, 8.2.3 and 8.2.4 where the insureds systems were adequate) were not PI losses. In drafting the endorsement, we have taken the position not to make a distinction in respect of the suitability of the IT systems used by the insured; there does not appear to be any clear guidance on this and the distinction was likely to lead to policy disputes. On balance and for consistency we decided to follow the approach taken by the majority of practitioners to all but one of the scenarios – and losses for breach of data protection are excluded under the clause (see 8.2.1 above for additional commentary).

Scenarios 9.1 – Mitigation Costs (forensic expenses)

The issue of mitigation costs in a scenario such as the misplaced laptop is quite difficult to address as the overriding view from survey respondents appears to be that liabilities to third parties arising from the loss should be covered by the PI but the data breach related costs to mitigate any loss should not be. Forensic costs would normally, we think, be dealt with in the incident response and privacy liability insuring agreements under a cyber policy. Moreover, we think that the respondents to the survey likely attached the provision of such costs to a breach of a Data Protection Law (as defined in the endorsement) and therefore should be excluded. However, there may be an argument that, in the example of sensitive client data potentially being lost, the forensic costs might be to mitigate losses for tort or breach of contract – in this case, possible third party claims for breach of confidentiality/privacy. If this is the case, the exclusion in the endorsement may not be triggered, but will be fact specific.

Scenario 9.2 on notification costs would, we believe, be excluded by paragraph 5 of the exclusion.

ENDS

See Annex 1 and 2 below.

ANNEX 1

PROFESSIONAL INDEMNITY CYBER AND DATA PROTECTION LAW ENDORSEMENT

1) This endorsement takes priority over any other provision in this contract.

2) Save as expressly provided in this endorsement, or by other restrictions in this contract specifically relating to the use of, or inability to use, a **Computer System**, no cover otherwise provided under this contract shall be restricted solely due to the use of, or inability to use, a **Computer System**.

3) This contract excludes any loss, damage, liability, claim, costs, expense, fines, penalties, mitigation costs or any other amount directly caused by, directly resulting from or directly arising out of:

   a) a **Cyber Act**; or

   b) any partial or total unavailability or failure of any **Computer System**;

   provided the **Computer System** is owned or controlled by the insured or any other party acting on behalf of the insured in either case; or

   c) the receipt or transmission of malware, malicious code or similar by the insured or any other party acting on behalf of the insured.

4) This contract excludes any loss, damage, liability, claim, costs, expense, fines, penalties, mitigation costs or any other amount directly or indirectly caused by, directly or indirectly resulting from or directly or indirectly arising out of any failure or interruption of service provided:

   a) to the insured or any other party acting on behalf of the insured by an internet service provider, telecommunications provider or cloud provider but not including the hosting of hardware and software owned by the insured;

   b) by any utility provider, but only where such failure or interruption of service impacts a **Computer System** owned or controlled by the insured or any other party acting on behalf of the insured.

5) This contract excludes any loss, damage, liability, claim, costs, expense, fines, penalties, mitigation costs or any other amount for actual or alleged breach of **Data Protection Law** by the insured or any other party acting on behalf of the insured.

6) Any cover for costs of reconstituting or recovering lost, inaccessible or damaged documents owned or controlled by the insured or any other party acting on behalf of the insured in this contract shall not apply to **Data**.

For the purposes of this endorsement the following definitions apply:

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.

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**.

Data means information, facts, concepts, code or any other information of any kind that is recorded or transmitted in a form to be used, accessed, processed, transmitted or stored by a **Computer System**.

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).

ANNEX 2 – Summary Scenario Analysis

Scenario	Survey: PII?	Who said 'PI?	Endorsement follows survey?
1.1 (1st Party) Theft Via Cyber Hacking (Hacker Steals Directly)	No	0%	Yes
1.2 (3rd Party) Theft Via Cyber Hacking (Hacker Steals Directly)	No	34%	Yes
1.3 (1st Party) Theft Via Cyber Hacking (Hacker Changes Details, Leads to Wrong Payment)	No	3%	Yes
1.4 (3rd Party) Theft Via Cyber Hacking (Hacker Changes Details, Leads to Wrong Payment)	No	40%	No
1.5 (1st Party) IP Theft Via Cyber Hacking	No	0%	Yes
1.6 (3rd Party) IP Theft Via Cyber Hacking	Yes	56%	No
1.7 Employee Involvement Changes Responses?	No	N/A	Yes
2.1 (1st Party) Mandate Fraud (Social Engineering)	No	7%	Yes
2.2 (3rd Party) Mandate Fraud (Social Engineering)	Yes	62%	Yes
2.3 (1st Party) CEO Fraud (Phishing)	No	4%	Yes
2.4 (3rd Party) CEO Fraud (Phishing)	Yes	58%	Yes
2.5 Hack Involvement Changes Responses?	No	N/A	Yes
3.1 Malware Spreading to Clients	No	24%	Yes
4.1 Virus Spreading to Clients (Insured a Marketer)	No	44%	Yes
4.2 Hacker Writes Libellous Posts on Client Account (Insured a Social Media Agency)	Yes	51%	No
4.3 Hacker Writes Defamatory Posts about Insured on Insured's Account	No	4%	Yes
5.1 (1st Party) Business Interruption from Ransomware	No	0%	Yes
5.2 Liability for Client Loss from Failure to Give Advice (Such Failure due to Ransomware Event)	Yes	75%	Yes
6.1 Reconstitution of Destroyed Confidential Client Data Held Electronically (Destruction Caused by Hack)	No	36%	Yes
6.2 Accidental Email of Confidential Data to Incorrect Third Party	Yes	97%	Yes
7.1 Professional Error due to Corrupt Professional Software	Yes	88%	Yes
8.1 GDPR - Professional advice causes breach of GDPR (insured's client's data was stolen)	Yes	92%	Yes

Scenario	Survey: PII?	Who said 'PI?	Endorsement follows survey?
8.2.1 GDPR - 3rd party financial losses from breach of suitable systems (no negligence by the insured)	No	12%	Yes
8.2.2 GDPR - Mandatory compensation payments for breach of suitable systems	No	8%	Yes
8.2.3 GDPR - ICO investigation and defence costs for breach of suitable systems	No	15%	Yes
8.2.4 GDPR - ICO fines for breach of suitable systems	No	8%	Yes
8.3.1 GDPR - 3rd party financial losses from breach of unsuitable systems	Yes	57%	No
8.3.2 GDPR - Mandatory compensation payments for breach of unsuitable systems	No	37%	Yes
8.3.3 GDPR - ICO investigation and defence costs for breach of unsuitable systems	No	39%	Yes
8.3.4 GDPR - ICO fines for breach of unsuitable systems	No	27%	Yes
8.3.5 Civil or negligence basis for GDPR	N/A	N/A	The endorsement does not make any distinction in this regard
9.1 Mitigation costs for laptop on a train; no sensitive data lost – forensic costs	No	19%	Possibly (fact specific)
9.2 Mitigation costs for laptop on a train; sensitive data lost – notification costs	No	24%	Yes
9.3 Mitigation costs for laptop on a train; sensitive data lost – hack involvement change response?	No	2%	Yes