FOIL
FORUM OF INSURANCE LAWYERS

Informing Progress - Shaping the Future

FOIL UPDATE 24th June 2021

Essex CHAMBERS

Hawkins 40 YEARS
Leaders in forensic investigation 1980 • 2020

Question Time on Silent Cyber

This event, held on 22nd June 2021, was hosted by the FOIL Technology & Cyber SFT and led by **Cameron Carr** of **DAC Beachcroft**.

'Silent cyber' or 'non-affirmative cyber' refers to the potential cyber exposures in non-stand-alone cyber policies, which may not be implicitly or explicitly included or excluded on policy wordings. Since about 2017, following regulatory activity from the PRA, and a subsequent mandate from Lloyd's in respect of cyber language, insurers have become increasingly focused on ensuring that cyber risk is properly addressed. There have been a number of bulletins issued to the Lloyd's market requiring policies to be clear as to whether cyber is, or is not covered.

The impact on drafting policies has been substantial and this event provided the opportunity for a wide range of experts to exchange views and deal with the questions raised. The panel comprised:

Graham Walsh – Senior Policy Adviser – ABI

Tom Hughes – Senior Market Services Executive - International Underwriting Association

John Pennick – Berkeley Insurance Group and British Insurance Brokers' Association

Simon Robinson – Claims and Insurance Director – FirstGroup PLC

Bob Still – Claims Manager – Entain Group

Question 1

'A report by the ABI on 2019 revealed that 99% of all claims made under ABI member cyber policies were paid, so, what is the problem?'

Graham Walsh

These figures may be misleading, as they relate only to affirmative cyber cover and not cover for silent cyber under other policies. It is also important to note that data collection is always a problem with cyber. The ABI has many members dealing with cyber policies but the level of submissions of data to the ABI has been inconsistent. Steps are currently being taken to refresh the data with cyber members to improve the quality, including in relation to claims paid and premiums. Better data is also needed to understand the solid cyber aspect of insurance, where no meaningful level of data has yet been collected.

Tom Hughes

The ABI figures are valuable in that they show what the stand-alone cyber market has been doing very well, i.e., supporting customers and paying claims. There are benefits to SMEs in having a standalone cyber policy, including the pre-inception discussions with the insurer about how to bolster their cyber security, the confidence that there is coverage and a support network if there is a loss.

The challenge that remains is the limitations of cyber coverage in traditional markets. Additionally, very few businesses have a stand-alone cyber product, with only about 6% of UK PLCs having such cover. Interest in cyber cover fell during the pandemic, even though the risk during that period probably increased with the shift towards home working, with less secure IT systems. Interestingly the same is not true in all jurisdictions and the opposite was seen in the German market, where demand for stand-alone cyber policies actually increased.

John Pennick also commented that the take-up of cyber cover is still relatively low, particularly amongst SMEs. Cyber risk means different things to different people and the range of cover available in the market on a stand-alone basis does vary. At one end of the spectrum people are buying limited cover for not a lot of money, but at the other companies are purchasing more comprehensive cover, including against cyber-crime. Knowledge of the nature of cyber risk has grown, compared to say five-ten years ago.

Simon Robinson looked at this issue from a policyholder's point of view. He is always pleased to see high rates of claim payments however accepts that insurers need fair premium for what they are covering so that they are around for the long term, providing consistency and not dropping in and out of the market.

Bob Still confirmed that his company has significant cyber risk. He is seeing changes in the available provision, as capacity seems to be reducing. Silent cyber has caused a lot of problems in the market, particularly from the point of view of whether or not something is covered.

Commenting further on capacity, **Tom Hughes** said that it was difficult to compare stand-alone cyber cover and cyber coverage in the traditional market, as coverage was not like-for-like. For example, an aviation policy with limits in the billions of dollars could simply not be replicated in the

stand-alone cyber market. For these reasons, in this example, it is for the aviation market to address cyber issues impacting upon its insureds, in order to continue to provide a valuable solution for their clients. Capacity in the traditional markets has not changed drastically, though we are now seeing some market hardening, with insurers understanding their obligations to adequately address new and rapidly changing risks. The PRA has been monitoring the situation for some time, as insurers develop their responses to these new exposures. Insurers recognise the need to ensure that they are adequately capitalised and there for the long term. We are in the midst of a significant change in policy language.

After **Cameron Carr** had listed just a few of the recent types of cyber risk that had been in the news, including cyber-attacks, ransomware, and solar winds, **Graham Walsh** agreed that there is a hardening in the market, not just in pricing but in insurers re-evaluating the risks they are taking.

Bob Still asked whether this hardening market was the result of insurers experience of silent cyber, where they have found themselves dealing with claims, which they probably had no intention to cover.

From the broking perspective, **John Pennick** thought that we are moving to a market that is more mature. There is more sophistication in underwriting. As far as the more traditional market is concerned, he was not aware of the pressures of cyber claims being a driver. His focus, however, has always been on the stand-alone side of the market, where there have been increases in areas such as ransomware and fraud.

Tom Hughes spoke about the regulatory angle. The PRA have made it clear that they are expecting insurers to identify, quantify and manage cyber risks. Lloyd's and others have driven forward new policy language. It is recognised that technology is now a part of everyday, as well as business life. That introduces a network of possibilities. Insurers are faced with a significant task, in not only considering the impact of cyber risk on an individual insured, but analysing their international portfolios, with clients of all sizes and across a wide range of industries.

Question 2

'Is silence in respect of cyber risks still acceptable?'

John Pennick thought that silence is not acceptable at all but the challenge for brokers is to work with clients to quantify what the risk is and what gaps there may be between stand-alone cover and what might have been covered under non-affirmative cyber cover, and whether there is a market solution for items that fall between. For a lot of SMEs, the challenge for BIBA members is raising their knowledge and understanding of cyber risks, which are changing all of the time. While ransomware is a topic at the moment, there could be greater risks that have yet to emerge. Brokers must appreciate how cyber risk dovetails with traditional property risks and then understand what a stand-alone cyber policy actually covers. The stand-alone cyber policy is not a panacea. Work is needed to produce cyber cover for as many situations as possible.

Simon Robinson agreed that silence is not acceptable. There needs to be openness from both sides as to what is and what is not covered. Affirmative cover is the way forward and he has seen silent cover removed across some sectors of his company's business, to be replaced by sub-limits or blanket exclusions. This has not been reflected in reduced premiums.

Bob Still sees silent cyber as a grey area of policy cover. While there have been grey areas in cover before, the cost of cyber claims can be so significant that grey areas need to be removed. Companies need affirmative cover, so that people like him can explain to the board exactly what is being done about risk transfer. Insurers seem to be learning pretty quickly what can and what can't be done. Having cover without silent cyber is essential for companies like the speaker's.

Graham Walsh commented that from the insurers' point of view, they must understand the risks they are carrying. From a customer perspective, openness and transparency are essential. The potential for conflict must be avoided between what is and what is not covered. Markets change all of the time and just because risks are excluded does not mean that premiums will necessarily go down. In some cases, insurers are simply revaluing risks they have been carrying.

Question 3

'How has the Lloyds' initiative on silent cyber changed the market practice?'

Tom Hughes explained that the Lloyd's Affirmative Action Plan requires syndicates providing coverage in Lloyds to clarify coverage, at policy level, in respect of both malicious and non-malicious cyber risk. The word 'affirmative' does not necessarily mean that cover will be provided, as there are a range of options for insurers to address cyber risk. There could be a broad positive affirmation to cover or continue to cover cyber risks, or there could be a broad exclusions and a range of potential options in between, such as write-backs, add-ons or sub-limits. The action plan has been a very positive exercise in producing a significant change in the market's wordings approach around cyber. Historically, there was a lack of consistency and understanding in respect of cyber, reflected at a policy level, now key cyber terms and definitions are used widely across a broad range of classes of business, namely: Cyber Incident, Cyber Act, Cyber Loss, Computer System and Data. The action plan began on 1st January 2020 (Phase 1) and by 1st July 2021 (Phase 4), all Lloyd's policies will need to contain cyber specific language. A range of model clauses has already been developed.

Although this is a Lloyd's initiative, it has wider ramifications, as it crosses over to the wider London market, through dual-stamp insurers who are active in both. These insurers appear to be utilising identical approaches across their Lloyd's and Company Market platforms.

The IUA has contributed to the debate about wordings, so far in the environmental liability and professional indemnity space. There are at least 160 model cyber clauses out in the market, with a range of variants to those clauses now being developed as brokers seek to negotiate on behalf of their insureds and tailor language to suit individual policyholders. These policy wording developments do create challenges, as each individual variant must be considered by an insurers legal and wordings team in order to understand how it differs from the model clause.

Broadly, the Action Plan has accelerated activity in respect of non-affirmative cyber risk as with each wording development an insurer must meet other fundamental requirements simultaneously, for example, understanding the inherent risk present, considering systemic exposures on a cross-class basis and ensuring they are adequately capitalised to respond.

Graham Walsh believes that, on the whole, there has been a very positive reaction to the Lloyds initiative. A few problems have emerged with some of the insurance lines, where the type of policy does not fit easily with what Lloyds are trying to do.

John Pennick had not yet experienced any problems with wanting to amend model wording but has found that the exercise has brought the focus onto cyber risk. The tendency has been to recommend stand-alone cyber risk cover but the problem is where that policy has exclusions that still expose the client to risk. For example, whereas before something might have been covered under property and casualty silent cyber, such as property damage caused by a malicious cyber act, that will probably not be covered under a stand-alone cyber policy. The conversation with the client now is about whether that cover can be obtained in the market. Identifying and trying to quantify cyber risks with clients has become a positive gain from this process and aids the process of presenting this to an underwriter, bearing in mind the requirements of the Insurance Act.

The speaker believes there is room for innovation in the market.

Simon Robinson was of the view that different parts of the insurance market are at different stages in the field of cyber risk and this was leading to some inconsistency, particular in relation to reinsurance. This also makes the comparison of quotations more difficult. This is less of a problem at the primary level.

Bob Still has experienced significant updating and clarification from insurers in relation to cyber cover (or lack of it), on an international basis. That assists in removing grey areas.

Tom Hughes

This process will inevitably take time. The IUA's underwriting committees have been talking about this subject for probably four or five years and, even now, understanding is continuing to grow. Tom agreed that some types of policy throw up challenges when clarifying cyber coverage, such as 'all risks' policies, which respond to an outcome without listing a range of covered perils; in these circumstances ambiguity can actually be brought by singling-out cyber as a peril, but not doing so for any other peril. International programmes can also throw up challenges, as other jurisdictions may not have the same regulatory requirements as the PRA, which may be one or two years ahead in its activity around cyber risk. It can be difficult to explain to an international broker or client the need for cyber language at a policy level, when they are not subject to the same regulatory conditions.

An example of positive collaboration between parties to further understand cyber risk was shown in the IUA's work in respect of professional indemnity. The IUA issued a survey to the market with a range of cyber scenarios, asking insurers, brokers and legal representatives to provide their opinions as to whether a professional indemnity policy should respond in the various circumstances. This process enabled model clauses to be drafted that seek to draw a line as to where a professional indemnity policy stops and where a stand-alone cyber policy starts. Clearly, model clauses are only models and are subject to alteration and do not have to be adopted.

John Pennick sees the challenges for the future for his members, in addressing non-affirmative cyber, as being able to have a sophisticated conversation with clients who understand cyber risks but who traditionally have not been called upon to do so.

For some the risk will mean protecting their computer network; for others it will be computer enabled fraud; for others a large-scale data breach. The policyholder needs to understand what the risk is; how it could affect them; and what is capable of being insured. At present, cyber risk means different things to different people. Brokers and insurers need to be agile but simplifying the identification of risk is important for the future.

Question 4

'What additional steps can the market take to ensure there are no unexpected coverage gaps on cyber?'

Simon Robinson recognises the need for blanket exclusions to bring the consistency and discipline an insurer needs. However, he would prefer more of a dialogue with the insurer about how the policy can best be written to work for his company: feeling that the insurer is working in partnership.

There should also be hypothetical discussions about whether or not, in a given scenario, the loss would be covered. These assist the policyholder to nail the insurer down on some issues.

Bob Still would like to see more capacity in the market. He also believes that insurers should work more closely with businesses to identify what is a cyber risk and what information insurers really need to offer cover. Both sides need to work much harder on this, well in advance of renewal.

John Pennick believes the market is moving in the right direction in having exclusions in all types of non-cyber insurance policies, where there is any non-affirmative cyber cover. Everything will then be picked up by stand-alone cyber insurance and where the underwriters fully understand and can properly quantify the risks, based on the data they will have collected. This will also address some of the gaps that are emerging from other types of policy.

Graham Walsh agreed that claims data was bound to assist underwriters but he felt that this is still a developing market which is some way from maturity. There is a good deal of work yet to be done on defining and refining what insurers offer.

Tom Hughes agreed with a point made by the previous contributor, that the BI test litigation had emphasised the importance of clarity in policy wording. He was less confident that blanket exclusions would emerge across non-stand-alone cyber classes to bring the focus onto stand-alone policies. Currently there are limitations in the stand-alone market relating to capacity and also non-cyber expertise. Expertise of stand-alone cyber underwriters needs to be married with expertise of traditional classes underwriters to understand the various nuances of policy operation and insured activities, applying cyber understanding to those non-cyber classes, so that cyber risks can be fully understood.

The speaker agreed that there must be more dialogue between insurers, brokers and policyholders to promote clarity in cover.

Q&A

Home working can increase cyber risk, but it depends on how workers are connecting into the system and what protections are in place. It is more of a threat where individuals are using their own devices and/or security software is breached.

information in this publication is accurate, all liability (including liability for negligence) for any loss and or damage howsoever arising from the use of this publication or the guidance contained therein, is excluded to the fullest extent permitted by law.