Justin Tivey Legal Director
justin.tivey@wbd-uk.com

Jonathan Drake Partner
jonathan.drake@wbd-uk.com

Womble Bond Dickinson LLP, Southampton & London

Looking ahead at the development of the United Kingdom's cyber insurance market

Justin Tivey and Jonathan Drake, of Womble Bond Dickinson LLP, assess the UK's developing cyber insurance market in the context of the changing regulatory landscape and assess the possible benefits and risks associated with the proposal to share data breach information between insurers and the ICO.

Cyber insurance is a hot topic and it is often described as a new and developing area. While it is certainly developing fast it is also the case that it has been around for longer than many imagine. Many date the first cyber policy to 1997 in the US. To put that in context in 1997 it is reckoned that around 1.7% of the world's population had internet access. Fast forward 20 years and by June 2017 that figure is over 50%.

The first cyber policy offered third party liability cover against breaches perpetrated by outsiders i.e. hacking - and nothing more. It was issued by one insurer and was a significant step at the time. Now as well as third party attacks cover can include the actions of employees and accidental data breaches as well as malicious ones. Cover for first party losses is obtainable and is in fact more likely to be called upon than the third party cover.

The number of insurers offering cyber cover on the London market is growing steadily. Historically insurers with a strong US presence or a US parent led the way but that is less the case now. Lloyd's of London reports 77 cyber risk insurers and in the Companies Market some form of cyber offering is widespread. Finally it seems so obvious as to be barely worth mentioning that information technology now runs through almost every aspect of daily life in business and in our homes. The ability to process data is fundamental and the effect of a loss of security in that data can range from irritating to very costly.

Despite this many surveys and comments by market insiders suggest that the take up of cyber cover is still relatively low and that cyber can be a hard sell. Anecdotally potential insureds can be put off cyber insurance by the confusing variety of wordings and scope of cover, its cost and an insufficiently clear understanding of what the benefit of the cover would be.

This all gives rise to some interesting questions: is the ability to assess cyber security risk mature enough yet? Will the General Data Protection Regulation ('GDPR') and the Network Information Security ('NIS') Directive aid the development of the market? And is the possibility of sharing information about cyber security breaches to be welcomed?

Is the ability to assess cyber risk mature enough yet?

As the short history of cyber insurance suggests, a number of carriers have been active in this area for some years and their experience has grown considerably. There is an understanding of how a book of such risks can perform and the perils and pitfalls that await the unwary.

The market certainly seems able to assess cyber risk and the range of cyber cover available supports this view. The fact that there are different levels of cover aimed at different types of insured and based on different policy wordings suggests that insurers are individually assessing what risk they can accept so that prices can be quoted and the deployment of underwriting capacity and the exposure of insurers' capital justified.

Some aspects of cyber liability are also clearly capable of being assessed and quantified. There is experience now of the costs of remediating a data breach and the likely cost of IT consultants, lawyers, public relations advisers and credit monitoring firms. The business interruption element of first party cyber cover is similar to that built into property damage cover for fire and flood. In most cases restoring IT systems will be quicker than dealing with fire or flood damage.

The financial liability of an insured to individual data subjects has not been considered in detail by the courts but there have been some relevant decisions which enable the potential liability to be estimated.


Image: Raphael Koh / Unsplash.com

Key facts about an insured can be ascertained, for example by asking what type of data they hold, what volume of data is held and in what format, where it is held and how is it protected. The type of insured, the size of the business and the number of employees is also more mundane but highly relevant information which affects the level of cyber exposure.

What is much more difficult is the assessment of the likelihood of a data breach incident occurring in any given year. However experience is developing all the time.

Insurers therefore seek to manage risk by putting in place policy sublimits, excluding certain higher risk events, applying a higher claim deductible and pricing the risk accordingly. The scope of cover for data breaches is measured in time and not just money, so breach support or business interruption cover may kick in after the insured has had a few hours to resolve the problem, thereby limiting exposure to more minor glitches or problems which have a readily identifiable solution or minimum impact.

Cover may end after a set period of time and retroactive dates are more common to limit the exposure to historic issues as well.

Insurers can opt to participate in cyber risks as part of the following market or on excess layers at higher levels of cover as they build up expertise.

That does not mean that there won't be surprises. Aggregation of risk is an area of concern. How easy would it be for one global attack, similar to the WannaCry incident of May 2017, to affect diverse insureds triggering multiple claims across a book of business?

As a growth area there continues to be a good flow of new insurer entrants into the market. This tends to drive down prices as insurers seek to build a book and compete for business. There can also be a temptation for insurers to enter the market without enough background preparation to gain a foothold in the market so as not to miss out.

Finally there are pressures from insureds for quotes to be given on the basis of only the briefest, and therefore probably inadequate, cyber related disclosure.

Away from the cyber market there is justifiably more concern about 'silent cyber;' the risk of policies not intended to cover this exposure picking up liability claims or possibly property damage resulting from a cyber incident.

To come back to the question - yes, the ability to assess cyber security risk is mature. Of course very few insurers would not want the benefit of having more information about the cyber risk environment, and there is lots of room for the market to mature further. The Prudential Regulation Authority's July 2017 Supervisory Statement about cyber highlights the steps insurers should be taking to actively consider their exposures to cyber risks and is a clear statement of good practice in this area.

Will the GDPR and the NIS Directive aid the development of the market?

The development of insurance markets is driven by many different factors, including customer awareness of risk and the availability of insurance to address it, and the perceived cost and benefit. The availability of capacity and broker support and involvement in the market are also important.

Outside of the industry regulatory and legislative changes can also play a large part in stimulating the market. Compulsory insurance is the most obvious example but regulation and legislation often increase or make clearer responsibility, liability and therefore risk of repercussions if things go wrong. This has helped

[Some] commentators say that cyber risk is so diverse, and changes more rapidly than other risks, that a different approach and a greater degree of voluntary information sharing could be justified.

continued

promote professional indemnity and D&O cover to more businesses than just the traditional professions.

Cyber insurance is no different in that regard and the GDPR' and to a lesser extent the NIS Directive will undoubtedly have an effect on the market.

The GDPR is law already but comes into operational effect on 25 May 2018 as it has a lead in time built into its provisions. The GDPR enhances the data protection regime across the EU and takes the existing data protection regime and broadens it. The UK Government has stated that it will remain UK law after Brexit. The maximum fines that regulators such as the UK's Information Commissioner's Office ('ICO') can impose have caught the headlines (up to 4% of global turnover) but crucially data processors as well as data controllers will be liable for breaches of the data protection regime. There is also a new general requirement to notify the ICO of serious data breaches. The requirements around obtaining data legitimately and the rights of citizens to have their data processed appropriately, have it protected and on request deleted, have all been enhanced. Liability is being incrementally increased and made to apply to a much larger group of businesses. A lot more businesses will have a bit more exposure than before. Cyber policies can address some of the resulting exposures - in particular liability to data subjects and contract disputes between processors and controllers when data breaches occur.

The NIS Directive requires EU Member States and operators of essential services to take appropriate security measures in respect of critical infrastructure. Member States must set up computer security bodies and identify essential service operators. These operators are obliged to maintain a specified level of security and to notify any security incidents. Essential services include energy, transport, water, banking and financial markets, healthcare and digital infrastructure providers. The NIS Directive comes fully into effect by November 2018 and again is intended to survive Brexit.

Logically these measures would boost the pool of businesses which need to think about their data risk and for whom cyber insurance could be a benefit. It should therefore increase interest in cyber cover and push up demand. This may also have the effect of increasing the price of cyber cover.

However the market is not driven by quite so simple an equation, and we often hear that there is an information requirement around the development of the market. There appears to be a need to educate potential buyers of cyber cover about the risks they run and how insurance can help manage those risks. Brokers will have a part to play in being able to explain these issues to insureds and help them to obtain appropriate cover. There is now pressure to standardise wordings. The availability of re-insurance is also a significant factor in making capacity available.

The education piece is not a new issue and there has been a learning curve for buyers of cyber cover, brokers and insurers alike. The GDPR and NIS Directive will boost interest and, it is to be hoped, help move everyone further up the curve.

What are the benefits and risks of sharing data breach information?

The ICO recently held preliminary discussions about data sharing with the Cyber Risk & Information Forum ('CRIF'), including representatives of some cyber insurers. Under one proposal, cyber insurers would provide data breach information which would then be aggregated and anonymised. This could include the type of breach, its scale, the type of insured and how long the breach took to be detected and resolved. This information would be shared with insurers and the ICO so that historical data would become available to more people more quickly. Interestingly, based on some reported comments, not all insurers welcome the idea.

Those insurers which have already built up knowledge about the incidence of cyber risk could lose their current competitive advantage if that type of information becomes more widely known. Others also question what the benefit is to the insurance industry in giving a regulator access to otherwise commercially sensitive information. From a legal perspective, information sharing across an industry also has to be handled carefully so that it does not contravene competition law. There are obvious potential benefits to sharing data. More data should mean better understanding of the frequency and level of incidents, which is one of the more difficult parts of the assessment of risk. It would also enable the ICO to see trends and perhaps focus its regulatory spotlight on those issues. This could improve risk for insurers.

Although there are already some databases of cyber incidents, a lot of this is actually publically available information albeit helpfully collated and searchable. The ICO/CRIF discussion would involve the sharing of a pool of data which would otherwise not be publically known. Other commentators say that cyber risk is so diverse, and changes more rapidly than other risks, that a different approach and a greater degree of voluntary information sharing could be justified, at least until the benefits of doing so can be better evaluated.

The cyber insurance market is older than many appreciate but is still a relative newcomer. With evolving cyber threats and a developing regulatory landscape, the perception of constant change seems unlikely to lessen any time soon.