GB Cyber Insurance Market Update H1 2021

The cyber insurance market has continued to evolve during the first half of 2021. We have seen an overall increase in the number and sophistication of attacks with a surge in ransomware attacks and claims. This has been further exacerbated by the COVID-19 outbreak which accelerated the shift to remote working with even more reliance on digital technology for business and so many other functions.

The changes in the overall cyber risk environment have had a rapid and dramatic impact on the cyber insurance market in several ways. Within this update we have set out the impact across 4 key areas being:

- Cyber insurance market capacity
- Claims & notifications
- Premiums & retentions
- Policy coverage

Cyber insurance market capacity (Reducing)

During the first half of 2021 the total capacity available in the **UK cyber insurance market has reduced**. This is due to several factors including: significantly increased claims activity; concerns around the **uncertainty in the overall cyber risk environment**; and the **potential for aggregation** of exposure across Insurers' portfolios (e.g. across industry sectors, geographies or through third party service providers).

As a result of these concerns, we have seen **limited new capacity** entering the UK market with the majority of existing cyber Insurers' looking to **reduce the capacity** that they will offer with a tighter focus on risk selection and a requirement for increased underwriting information. Increasingly, Insurers' are only willing to provide capacity on risks which fit exactly within their underwriting appetite.

With the market in a state of flux, we have seen a degree of **volatility with Insurers' strategies** which are often subject to short notice changes, making it challenging to navigate.

From a Lloyd's of London perspective we are already learning of certain Lloyd's syndicates paying **close attention to the volume of premium they have written** in the first half of the year in order not to breach their stamp capacity (the amount of premium they are authorised to write in an annual period) and ensure they have sufficient capacity available for their renewal business in the second half of 2021.

For **Cyber Physical Damage cover** - overall capacity is under similar pressure, although unlike traditional cyber cover the interest in primary/lead positions has been less impacted.

Due to the constraints in capacity, we are seeing a trend of insureds having to **retain more risk** on their balance sheet and/or through a captive, not only to mitigate the rate increases but to be able to maintain their programme limits, which in some cases are reducing form their expiring levels.

Claims & notifications (Increasing)

The **surge in ransomware events** which we saw in 2020 has continued to dominate in terms of the frequency of claims notifications and claims payments made. According to our Willis Towers Watson Ransomware Claims analysis (analyzing over 210 ransomware claims between 2017 and 2021), the largest share of claim costs following a ransomware event are the **payment of the ransom (37%)** and **resultant business interruption (18%)**. More recently, **data extraction** as part of a Ransomware event has introduced another level of costs in the form of **regulatory exposure** and longer-term liabilities. Whilst Ransomware events are affecting companies of all sizes across multiple industries and geographies, our Claims Insight Data shows that **worst hit sectors** in terms of ransomware attacks have been Healthcare, Manufacturing, Education and IT/Telecommunications.

Willis Towers Watson

In some countries Ransomware attacks have directly impacted critical national infrastructure, with the Colonial Pipeline being one of the most recent high-profile victims. As a result, the insurance market approach to covering Ransomware losses is under **scrutiny by regulators and at government level**.

Claims notifications regarding t**echnology supply chain issues** continue to arise, creating concern for Insurers' about their exposure to a global systemic event. Data gathered from our broader Cyber claims analysis (analyzing close to 1900 cyber claims dating back to 2013) shows that third party security breaches are currently responsible for 32% of data breach losses. The most recent attack against Kaseya, an IT and security management provider, is a good example of this exposure and follows the **SolarWinds, Microsoft Exchange** and **Accellion** attacks earlier in the year.

As a result of increased claims activity, Insurers' are more actively seeking to **manage overall claims costs** and expenses with a focus on third party incident response providers that a company may utilise following a cyber incident.

Premium & Retentions (Increasing)

In the first half of 2021 we have seen **premiums and rates continue to rise**, with Q2 seeing average increases in the region of 50% for risks without claims and with strong cyber risk management controls in place. For those clients with a claims history or weaker security controls these increases have been substantially higher.

Speaking in June 2021 a Chief Underwriting Officer of a leading Lloyd's of London insurer commented:

> **"In terms of cyber cover, we have seen an acceleration of rates," he explained. "In 2020, we saw rates at plus 10% - in the first quarter of this year it was plus 25% and at current renewals we are seeing plus 100%, as market capacity plateaus.[1]"**

Insurers' are increasingly **concerned about the underlying profitability** of cyber programs, following increased claims activity and are keeping a **close eye on their pricing models** in response. Their focus is on the overall **adequacy of premiums** relative to the exposure i.e. simplistically, will the premiums collected cover the expected claims.

In common with many commercial insurance lines, Cyber works on a layered basis and the premium increases being applied in the primary layers have led to reviews of the excess layers, with Insurers' seeking to ensure profitability, and as a result premium and rate increases are generally being applied across all layers.

The claims activity across insurer portfolios has also impacted on monetary retentions and time waiting periods with Insurers' increasingly looking to apply increases to manage lower level losses and give clients more 'skin in the game' albeit there are still variations based on many factors such as industry sector, size and exposures.

Policy coverage (Under review)

Due to concerns around the increased volume and cost of ransomware claims, some Insureds' **have imposed sub-limits** on ransomware coverage and are also **utilising co-insurance** (with the insured taking a proportion of the risk) to manage their exposure to this threat. Insurers' approach in this area is generally driven by the maturity of a company's cyber risk controls and processes, rather than changes being applied on a blanket basis.

A key element of cover for ransomware attacks is the payment of the ransom itself. Due to the increased frequency and severity of ransomware attacks, the ransom payment coverage is now a **focus at government level**.

Insurers' are also paying more attention to other coverage areas where they have had previous concerns. These include exclusions relating to: Critical Infrastructure, Natural Perils, War/Terrorism and BIPA (the Biometric Information Privacy Act regarding the informed consent of collection and storage of biometric data prior to its collection). We anticipate that further coverage restrictions could come into play in the second half of the year, particularly if the claims environment does not improve.

Coverage innovation cannot be completely ruled out, but there are a fewer number of Insurers' willing to be more creative in their approach to coverage.

Some policies offer combined cover for Cyber and Tech Professional Indemnity. Once again Insurers' are pulling away from offering these given the additional exposure and challenges arising from COVID-19. In several cases the increased demand for home working has highlighted potential weaknesses in IT Systems and weaknesses in remote access security controls, which could lead to a cyber-attack or breach. Reductions in project spend or project delays may also lead to contractual disputes for on-going projects.

1. https://www.insurancetimes.co.uk/news/london-market-told-to-maintain-pace-of-change-post-pandemic/1437952.article

Key issue: Underwriting information

Insurers have shifted their underwriting focus to **the level of technical controls and processes** which are in place and as we have mentioned, they must demonstrate more **diligent underwriting practices and careful risk selection. Ransomware controls** in particular have become critical to being able to maintain or secure cyber insurance coverage. Companies will need to provide **separate ransomware application forms** which outline the key controls and processes that need to be in place. We have set out below a **summary of the top 10 minimum essential areas** which must be addressed.

1. Do you utilise Multi Factor Authentication (MFA) across your network for ALL remote access and privileged admin access?
2. Do you employ an endpoint detection and response solution that is fully deployed across all endpoints?
3. Do you keep your back-ups separate from your primary network e.g. within a cloud service or data centre ("offline")
4. Do you regularly test the successful restoration and recovery of key server configurations and data from back-ups?
5. Do you have an encryption policy which requires the encryption of data and backups?
6. Do you segment your network (including network data) by business function and geography?
7. Do you have Advanced Technology for scanning and filtering of web and email traffic, including Firewall protections?
8. Do you keep all critical business systems securely configured and up to date with a process to rapidly deploy critical patches for vulnerabilities?
9. Do all employees receive training on phishing and other social engineering techniques?
10. Do you have a BCP (Business Continuity Plan) and/or a DRP (Disaster Recovery Plan) which is reviewed and tested annually?

Preparing for your renewal

- **Timing:** Start the renewal process earlier. The underwriting process is more detailed, internal insurer sign offs are often required and it's often necessary to seek options from alternative insurers. This will take additional time which must be built into the renewal timetable.
- **What's most important?** In the current market conditions, it is often difficult to get everything you want. Going into a renewal, having a clearer view of your key priorities, be that coverage, total limits, pricing or retentions, will enable a more flexible response to insurers' terms.
- **Anticipate what underwriters will want to know:** In the current market conditions the level and type of information which is seen as essential by underwriters has increased significantly. Understanding where underwiters are focusing will enable you to be prepared to respond to their questions and enable differentiation in key areas.
- **Engage with insurers:** Providing a detailed written submission and, where appropriate, giving access to the key individuals on the front line who manage the risk, will build confidence with insurers and enable a more streamlined approach answering questions.
- **Leverage your relationships:** Understand which insurers you have relationships with across other lines of insurance and use these to leverage your renewal discussions.

For more information

Glyn Thoms
Head of FINEX Cyber & TMT, FINEX GB
T: +44 203 124 8673
M: +44 7985 164 928
Glyn.Thoms@WillisTowersWatson.com

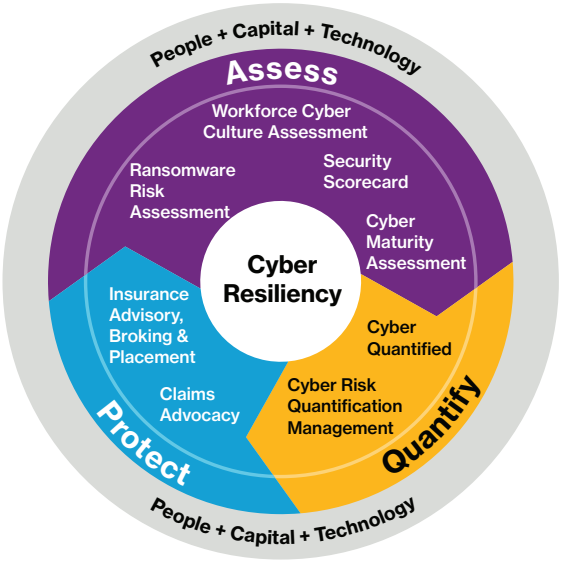
Willis Towers Watson offers insurance-related services through its appropriately licensed and authorised companies in each country in which Willis Towers Watson operates, for example:

- In the United Kingdom, Willis Limited, registered number: 181116 England and Wales. Registered address: 51 Lime Street, London, EC3M 7DQ. A Lloyd's Broker. Authorised and regulated by the Financial Conduct Authority for its general insurance mediation activities only; and
- Willis Towers Watson SA/NV, Quai des Vennes, 4020, Liège, Belgium (0415.981.986 RPM Liège) (registered as a branch in the UK at 51 Lime Street, London, EC3M 7DQ UK Branch Number BR021056) in relation to all EEA-regulated business. Authorised by the Financial Services and Markets Authority (FSMA) Belgium, and authorised and subject to limited regulation by the Financial Conduct Authority. Details about the extent of our authorisation and regulation by the Financial Conduct Authority are available from us on request.

For further authorisation and regulatory details about our Willis Towers Watson legal entities, operating in your country, please refer to our Willis Towers Watson website.

It is a regulatory requirement for us to consider our local licensing requirements prior to establishing any contractual agreement with our clients.

This publication offers a general overview of its subject matter. It does not necessarily address every aspect of its subject or every product available in the market. It is not intended to be, and should not be, used to replace specific advice relating to individual situations and we do not offer, and this should not be seen as, legal, accounting or tax advice. If you intend to take any action or make any decision on the basis of the content of this publication you should first seek specific advice from an appropriate professional. Some of the information in this publication may be compiled from third party sources we consider to be reliable, however we do not guarantee and are not responsible for the accuracy of such. The views expressed are not necessarily those of Willis Towers Watson.



About Willis Towers Watson

Willis Towers Watson (NASDAQ: WLTW) is a leading global advisory, broking and solutions company that helps clients around the world turn risk into a path for growth. With roots dating to 1828, Willis Towers Watson has 45,000 employees serving more than 140 countries and markets. We design and deliver solutions that manage risk, optimise benefits, cultivate talent, and expand the power of capital to protect and strengthen institutions and individuals. Our unique perspective allows us to see the critical intersections between talent, assets and ideas – the dynamic formula that drives business performance. Together, we unlock potential. Learn more at willistowerswatson.com.

willistowerswatson.com/social-media

FPS2103876 WTW-FINEX 487607/09/21

willistowerswatson.com

Willis Towers Watson